Revisiting the Robustness of (R/M)LWR under Polynomial Moduli with its Applications

Haoxiang Jin(✉)[1], Feng-Hao Liu[2], Zhedong Wang[3], and Yang Yu[4]

[1]University of Illinois Urbana-Champaign, jin56@illinois.edu
[2]Washington State University, feng-hao.liu@wsu.edu
[3]Shanghai Jiao Tong University, wzdstill@sjtu.edu.cn
[4]Tsinghua University, yu-yang@mail.tsinghua.edu.cn

Abstract

This work conducts a comprehensive investigation into determining the *entropic* hardness of (Ring/Module) Learning with Rounding (LWR) under polynomial modulus. Particularly, we establish the hardness of (M)LWR for general entropic secret distributions from (Module) LWE assumptions based on a new conceptually simple framework called rounding lossiness. By combining this hardness result and a trapdoor inversion algorithm with asymptotically the most compact parameters, we obtain a compact lossy trapdoor function (LTF) with improved efficiency. Extending our LTF with other techniques, we can derive a compact all-but-many LTF and PKE scheme against selective opening and chosen ciphertext attacks, solely based on (Module) LWE assumptions within a polynomial modulus. Additionally, we show a search-to-decision reduction for RLWR with Gaussian secrets from a new Rényi Divergence-based analysis.

1 Introduction

Lattice-based cryptography has attracted significant attention in recent years – first it stands out as one of very few promising candidates against quantum algorithms [Sho94], and moreover, it provides as a robust foundation upon which a wide array of (advanced) crypto systems can be built, e.g., [Pei16a]. Particularly, many lattice-based crypto systems are directly based on the *learning with error* (LWE) problem [Reg05], which enjoys search-to-decision reductions [Reg05, Pei09, MM11, MP12] and as well as worst-case hardness from some lattice problems, under quantum or classical reductions [Reg05, Pei09, BLP+13]. These results instill confidence in the hardness of LWE, encompassing both its decision and search forms, and consequently, in the security of cryptographic systems derived from LWE.

However the LWE problem requires to sampling random errors, leading to efficiency losses and complications in designing some cryptographic primitives that are deterministic in its nature of computation, e.g., pseudorandom functions (PRFs). To tackle these challenges, the work [BPR12] introduced the Learning with Rounding (LWR) problem as a derandomized version of the LWE. Then the research community identified that many crypto systems can be naturally derived from LWR, such as PRFs [BPR12] , lossy trapdoor functions (LTFs), reusable extractors, and deterministic encryption [AKPW13]. As these systems do not require Gaussian samplings, they are in general easier to implement and more efficient. To further improve efficiency, we can employ additional algebraic structures, such as Ring-LWR or Module-LWR, similar to the Ring/Module-LWE problem.

Robustness of LWR. Goldwasser et al. [GKPV10] initiated a study on the robustness of LWE, aiming to achieve an entropic notion of security that guarantees LWE hardness even if the secret only contains certain entropy. This notion has natural connection with leakage resilient cryptography and has many applications (see e.g., [KR19] for a survey). In the research of (Ring-Module) LWE, significant progress has been made [ACPS09, GKPV10, LPR13, AKPW13, BD20a, BD20b, BJRW22, LWZW24]. Particularly, [BD20a] (and [BD20b]) confirmed the hardness of entropic LWE (RLWE) for general entropic distribution, i.e. the secret has sufficient entropy.

However, for the case of (Ring/Module) LWR, current research remains unsatisfactory for the following reason:

- While it is possible to derive the hardness result of entropic LWR for general entropic distribution by combining the hardness result of [BD20a] with the simple reduction from LWE to LWR in [BPR12], this approach requires the moduli to be super-polynomial. Unfortunately, this parameter setting leads to worse efficiency and requires stronger assumptions on the underlying LWE problem (with super-polynomial modulus).
- To address these drawbacks, [AKPW13] (and [LW20]) showed the hardness of entropic LWR (Module LWR) with polynomial modulus, but their reductions only hold for bounded secret distributions, meaning that the secret must come from some small-norm distributions.
- For Ring-LWR with polynomial modulus, our understanding is limited – it remains unknown whether the output is pseudorandom if the secret comes from a norm-bounded distribution, particularly the Gaussian distribution.

These shortcomings hinder the applicability of current hardness results in analyzing the security of the crypto schemes in [AKPW13], which requires an entropic (Module) LWR for general secret distributions. Additionally, leakage resilience of some RLWR (or MLWR)-based PKE schemes is affected, as seen in early round submissions to the NIST's post-quantum cryptography call (e.g., [BBF+19, DKRV18]).

The above discussions highlight a gap between our comprehension in entropic (Ring/Module) LWE and that in entropic (Ring/Module) LWR. On one hand, the most effective attacks to LWR appear to be those designed for LWE. On the other hand, there are apparent technical barriers to establishing the hardness of LWR based on LWE within a polynomial modulus, as indicated in [NR23]. In an effort to advance the state of the art, this work is motivated to undertake a more refined exploration of entropic (Ring/Module) LWR, with a specific focus on the following objectives.

> (**Main Goal 1:**) Under polynomial modulus, determine the hardness of entropic (Module) LWR for general secret distributions, and the hardness of (decision) RLWR for Gaussian secrets.

Compact LTFs from Lattices. Lossy trapdoor functions (LTFs) are powerful crypto tools that can be used to construct many applications, such as trapdoor one-way functions, collision-resistant hash functions, lossy encryption, CCA2 secure PKE, etc, [PW08]. They can be extended to design the more advanced *all-but-many lossy trapdoor functions* (ABM-LTFs) [BL17, LSSS17], which can be used to realize PKE with a stronger notion of security, namely, *selective opening chosen-ciphertext-security* (SO-CCA security). For lattice-based constructions, there are several prior works [BKPW12, PW08, AKPW13, DGI+19], among which, the construction in [AKPW13] is conceptually very simple, based on entropic LWR.

However, all the prior schemes have some drawbacks across various aspects, including *information rate*[1], *lossiness*[2], and the *public parameter size*. For example, the constructions in [PW08, AKPW13] suffer from super-constant information rate, the work [BKPW12] achieves small lossiness parameter, and the work [DGI+19] requires very large public parameters and involves much complicated parallel repetition, leading to poor efficiency.

Recently, the work [HHK+24] designed a compact LTF ($O(1)$ information rate) based on lattice, and further extended the basic result to compact *all-but-many*-LTFs (ABM-LTFs) and *selective opening*-CCA (SO-CCA) secure PKE based. Despite the theoretical advancements, the designs in [HHK+24] are rather intricate, involving heavy Gaussian sampling, harsh restriction for achieving strong lossiness, and large public parameters compared to the very simple (though non-compact) [AKPW13]. Additionally, their ABM-LTF construction assumes the existence of a PRF computable in NC1 (taking the PRF key as input). While such a PRF can be instantiated from lattice [BLMR13], the construction requires a super-polynomial modulus. Consequently, it remains unclear whether the results of [HHK+24] can be derived from lattices under a polynomial modulus, which is a weaker assumption. These considerations motivates our second goal.

> (**Main Goal 2:**) Improve the state of the art of LTF constructions in [HHK+24] with a more conceptually straightforward and efficient design. Then determine whether we can eliminate the requirement of PRF in NC1 to achieve ABM-LTF and SO-CCA PKE under a polynomial modulus.

1.1 Our Contributions

This work aims at the two main goals and makes three major contributions.

Contribution 1. We establish hardness results for the general entropic LWR problem from the standard lattice-based assumption. In particular, we show a reduction from LWE to entropic LWR with general entropic secret distributions (i.e., which only require sufficient entropy over the secret). To achieve this, we propose a new measure called "*rounding lossiness*", and show that high min-entropy of a secret distribution implies (some level of) rounding lossiness. Moreover, we show that high rounding lossiness implies entropic hardness of LWR. Informally, our new hardness results can be summarized by the folloing theorem:

Theorem 1.1. *Assume that decision LWE is hard under poly-modulus q (and for other appropriate parameters). Let $\mathcal{S}$ be a distribution over $\mathbb{Z}_q^n$ with sufficient min-entropy, then Entropic LWR with secret distribution $\mathcal{S}$ is hard.*

This result generalizes the hardness results of entropic LWR in [AKPW13] from bounded secret distributions to general entropic distributions, and thus improves its applicability to other crypto designs as presented in [AKPW13]. In our second contribution, we present an important application to compact LTFs and generalizations. It is worth noting that this new reduction approach can also be adapted to the MLWR setting, deriving the hardness of entropic MLWR with any secret distribution that has sufficient min-entropy (*rounding lossiness*), from the hardness of MLWE (or RLWE). To the best of our knowledge, our reduction is the first result of the hardness of general entropic (M/L)LWR.

[1] Information rate is defined as the input-to-output ratio, with a higher value being preferable. A design is *compact* if the rate is $O(1)$.

[2] Lossiness is the parameter that quantifies the average number of bits lost when evaluating the function in the lossy mode. In our applications, a higher lossiness is desirable.

Contribution 2. We achieve our *Main Goal 2* for designing lattice-based LTFs, ABM-LTFs and SO-CCA secure PKE with a polynomial modulus, simultaneously achieving good compactness, lossiness and efficiency. This improves the state-of-the-art constructions of [HHK+24] as we elaborate below.

- Our basic LTFs follow the framework of [AKPW13], and enjoy the extremely simple construction: the public key is a matrix $\mathbf{A}$, and the function defined as $f_{\mathbf{A}}(\boldsymbol{s}) = \lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_p$ is just the evaluation algorithms of LWR. Based on our hardness result of entropic LWR in Contribution 1, we further enlarge the bounded input domain of LTFs construction in [AKPW13] to general entropic distribution over $\mathbb{Z}_q^n$, resulting in more compactness and lossiness we can achieve.
- We further reduce the information rate of LTFs in [AKPW13] to constant (can further approach 1 asymptotically), by designing a compact trapdoor inversion algorithm for LWR, which is compatible with the *lossy mode*[3]. The main technique contribution is a reduction from (HNF)LWE to a *special decision knapsack problem* under arbitrary modulus with asymptotically the most compact parameters (we further show its tightness via some novel number theory analyses). The crux of our reduction is a fine-grained analysis of the probability that random matrix over $\mathbb{Z}_q^{n \times m'}$ has an invertible sub-matrix for arbitrary modulus q, which has several other applications and should be of interest.
- We further derive constructions of compact ABM-LTFs and compact SO-CCA secure PKE with all building blocks that can be initiated with poly modulus.

Compared with the constructions in [HHK+24], our constructions have several significant advantages. Firstly, our basic LTF scheme is much simpler, due to the extremely simple evaluation algorithms of LWR. Secondly, the amount of "lossiness" in our LTF construction is more flexible. Particularly, we can achieve the *relative lossiness*[4] arbitrarily close to 1 with poly modulus rather than super-poly modulus in [HHK+24]. Next, our LTF is with smaller evaluation key, i.e., $O(n^2 \log q)$ for ours vs $O(n^2 \log^4 q)$ for [HHK+24]. Finally, our constructions of compact ABM-LTFs and compact SO-CCA secure PKE are with polynomial modulus without relying on the additional assumption of PRFs mentioned in [HHK+24].

Contribution 3. We prove pseudorandomness of RLWR with Gaussian secret from the standard assumptions over ideal lattices. Particularly, we first show a reduction from search RLWR with certain entropic secret distributions (with sufficient entropy) to decision RLWR with Gaussian secret distributions. To the best of our knowledge, this is the first hardness result that captures RLWR with bounded secret distributions. The crux is a Rényi Divergence (RD)-based noise flooding technique for matrix-vector multiplication (or multiplication of ring elements). As previous analyses mainly focus on the vector addition (or ring elements addition), our new analysis would be of independent interest. Informally, this hardness result can be summarized as follows:

Theorem 1.2. *Assume one-way hardness of RLWR with certain entropic secret distribution holds under* poly*-modulus (and for other appropriate parameters), then the decision RLWR with Gaussian secret distributions (defined according to coefficient embeddings) also holds.*

We note that establishing the hardness of RLWR with Gaussian-distributed secretes not only has intrinsic scientific significance but can also enhance the hardness of RLWR with centered binomial secrete distribution, which has been adopted by some RLWR (or MLWR)-based PKE schemes (e.g., [BBF+19, DKRV18]).

[3]The lossy mode is a necessary technique for designing LTFs from LWR in [AKPW13], and will be described in the part of technique overview latter.

[4]The measure of *relative lossiness* in [HHK+24] is to denote the ratio of the remaining entropy of the input and the original entropy of the input.

Particularly, in practical applications, the discrete Gaussian distribution can be replaced by the centered binomial distribution, without significantly compromising provable security (referring to [ADPS16,LLZ+18]).

We next generalize the search RLWE to search RLWR reduction in [LW20] to the case of entropic secrets, and thus establish the hardness of our special search entropic RLWR. Combining with the hardness results of entropic RLWE in [BD20b], the hardness of our special search entropic RLWR can be further established from the standard assumptions (e.g. RLWE and NTRU). Informally, we have the following corollary:

Corollary 1.3. *Assume the pseudorandomness of RLWE and NTRU holds under* poly*-modulus (and for other appropriate parameters), then the decision RLWR with Gaussian secret distributions (defined according to coefficient embeddings) is* $\frac{1}{\mathsf{poly}(\lambda)}$*-secure.*

It needs to point out that we cannot bridge the (strong) pseudorandomness (i.e. $\mathsf{negl}(\lambda)$-security) of RLWR with Gaussian secret distributions to the standard assumptions under poly-modulus. The main technique barrier is that there exists a lower bound for showing a sample-preserving reduction from RLWE to RLWR with polynomial modulus by a recent work [NR23]. Nevertheless, as mentioned in [LW20], this barrier for applications can be overcome via the hardness amplification technique of [Tes11].

1.2 Technical Overview

In this section, we present an overview of our techniques. Referring to the description of our main contributions, we highlight three interesting techniques in Contributions 1, 2 and 3, respectively.

1.2.1 Rounding Lossiness Approach to Entropic LWR

To start with, we need to propose a framework to handle the LWR with general entropic secrets, i.e., relate the hardness of Entropic LWR for general distributions to a basic property of the distribution. To this end, we propose a measure called *rounding lossiness*. Specifically, let $\mathcal{S}$ be some distribution over secrets in $\mathbb{Z}_q^n$, and the rounding lossiness of $\mathcal{S}$ is defined as $\mathcal{R}_{q,p^*}(\mathcal{S}) = H_\infty\left(\boldsymbol{s}|\lfloor \boldsymbol{s}\rceil_{q,p^*}\right)$, where s is sampled from $\mathcal{S}$ and $\lfloor \boldsymbol{s}\rceil_{q,p^*} = \left\lfloor \frac{p^*}{q}\cdot \boldsymbol{s}\right\rceil$ denotes the deterministic rounding of $\boldsymbol{s}$ with parameters q, p^*. It's easy to lower bound this conditional min-entropy by

$$H_\infty(\boldsymbol{s}|\lfloor \boldsymbol{s}\rceil_{q,p^*}) \geq H_\infty(\boldsymbol{s}) - \log\left(\left|\lfloor \boldsymbol{s}\rceil_{q,p^*}\right|\right),$$

where $|\cdot|$ denotes the size of a space here. The term $\log\left(\left|\lfloor \boldsymbol{s}\rceil_{q,p^*}\right|\right)$ can be upper bounded by $n\log p^*$ for general secrets or $n\log(\frac{p^*\cdot\gamma}{q})$ for γ bounded (under ℓ_∞ norm) secrets. This naturally bridges the entropy requirement of distribution and the *rounding lossiness* of distribution.

The following target is to deduce the hardness of Entropic LWR to the *rounding lossiness* approach. Our approach consults the reduction approach in [AKPW13]. We show a minor yet crucial modification of their approach that allows to relate the hardness of Entropic LWE to the *rounding lossiness* of the secret distribution. To explain more clearly, we first take a look at the proof framework in [AKPW13].

1. We first break $\mathbf{A} = (\mathbf{A}', \boldsymbol{a})$ where $\mathbf{A}'$ is the first $\ell - 1$ rows.
2. We switch $\mathbf{A}'$ into some lossy matrix $\tilde{\mathbf{A}}' = \mathbf{B}\cdot\mathbf{C} + \mathbf{F}$, where $\mathbf{B}, \mathbf{C}$ are uniformly at random, and $\mathbf{F}$ is an error matrix with bounded norm.
3. Then we show that the conditional entropy $H(\boldsymbol{s}|\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}'\cdot\boldsymbol{s}\rceil_{q,p})$ is still high.

4. Thus, from a leftover hash lemma we have $(\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q,p}, \boldsymbol{a}, \lfloor \boldsymbol{a} \cdot \boldsymbol{s} \rceil_{q,p}) \approx (\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q,p}, \boldsymbol{a}, \lfloor u \rceil_{q,p})$, as $\boldsymbol{a}$ acts as a fresh random seed.

5. We switch back $\tilde{\mathbf{A}}'$ to $\mathbf{A}'$.

We follow the same steps 1, 2, 4, 5 as [AKPW13], and modify the step 3 as follows:

- Artificially parse $\tilde{\mathbf{A}}' \cdot \boldsymbol{s} = \mathbf{B} \cdot \mathbf{C}\boldsymbol{s} + \mathbf{F}\boldsymbol{s} = \mathbf{B} \cdot \mathbf{C}\boldsymbol{s} + \frac{q}{p^*}\mathbf{F} \cdot \lfloor \boldsymbol{s} \rceil_{q,p^*} + \frac{q}{p^*}\mathbf{F}(\frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s} \rceil_{q,p^*})$;
- Based on step (1), $\lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q,p}$ can be reconstructed given $\mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \lfloor \boldsymbol{s} \rceil_{q,p^*}, Z$, where Z is the border space such that $\lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q,p} \neq \left\lfloor \mathbf{B} \cdot \mathbf{C}\boldsymbol{s} + \frac{q}{p^*}\mathbf{F} \cdot \lfloor \boldsymbol{s} \rceil_{q,p^*} \right\rceil_{q,p}$. Now determining $H_\infty(\boldsymbol{s} | \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q,p})$ can be deduced to determining $H_\infty(\boldsymbol{s} | \lfloor \boldsymbol{s} \rceil_{q,p^*})$;
- Bound the size of Z with overwhelming probability and determine the constrains of parameters.

The main difference between our approach and that in [AKPW13] is that instead of directly relating $\mathbf{F} \cdot \boldsymbol{s}$ to the border space, we relate $\frac{q}{p^*}\mathbf{F}(\frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s} \rceil_{q,p^*})$ to the border space. The infinite norm of $\frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s} \rceil_{q,p^*}$ (or $\boldsymbol{s}$ in [AKPW13]) determines the lower bound of modulus. It's clear that the upper bound of $\frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s} \rceil_{q,p^*}$'s ℓ_∞ norm is exactly 1/2. This is the main technical reason why our approach can achieve the hardness of Entropic LWR with general secret distributions.

It should be noted that the *noise lossiness* approach in [BD20a] can be implicitly used to analyze the hardness of general entropic LWR (need some subtle adjustments). Compared with the *noise lossiness* approach, our approach is conceptually simpler and enjoys better parameters. Therefore, for Entropic LWR, it's more advantageous to work with our rounding lossiness approach. For more detailed analysis of two lossiness model, we refer to section 4 and Appendix B.

1.2.2 Compact Trapdoor Inversion Algorithm

Next, we explain our design of compact trapdoor inversion algorithm for LWR. Our design follows the framework of [MP12, AKPW13], but with some modifications. We start to recap this framework and explain the motivation to achieve compactness:

- The trapdoor generating algorithm takes integers $n, m = m_1 + m_2, q$ as input, then uniformly samples $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{n \times m_1}, \mathbf{R} \xleftarrow{\$} \{-1, 1\}^{m_1 \times m_2}$ and outputs the public matrix $\mathbf{A} = \begin{pmatrix} \bar{\mathbf{A}} & \bar{\mathbf{A}}\mathbf{R} + \mathbf{G} \end{pmatrix}$ and the corresponding trapdoor $\mathbf{T}_\mathbf{A} = \begin{pmatrix} -\mathbf{R} \\ \mathbf{I} \end{pmatrix}$, where $\mathbf{G} \in \mathbb{Z}_q^{n \times m_2}$ is the gadget matrix with a public and short trapdoor.
- The trapdoor inversion algorithm for LWR inputs $\mathbf{A}, \mathbf{T}_\mathbf{A}$ and some vector $\boldsymbol{c} = \lfloor \boldsymbol{s}^\top \cdot \mathbf{A} \rceil_p$ for some $p \in \mathbb{Z}_q$, and outputs $\boldsymbol{s}$.

Intuitively, the LWR instance $\lfloor \boldsymbol{s}^\top \cdot \mathbf{A} \rceil_p$ can be treated as a special LWE instance, i.e., $\lfloor \boldsymbol{s}^\top \cdot \mathbf{A} \rceil_p = \frac{p}{q}(\boldsymbol{s}^\top \cdot \mathbf{A}) + \boldsymbol{r}$. Then one can apply the inversion algorithm for LWE ([MP12]) to find the secret $\boldsymbol{s}$ of LWR under certain parameters.

In an LWR-based LTFs ([AKPW13]), the input is the secret $\boldsymbol{s}$, the output is the vector $\lfloor \boldsymbol{s}^\top \cdot \mathbf{A} \rceil_p$, and the trapdoor inversion algorithm for LWR is the the inversion algorithm of LTFs. In this case, the ratio of $\frac{m}{n}$ highly determines the compactness of the construction, and smaller ratio (preferably constant) is desired. Thus, our target is to minimize this ratio. To achieve this, we need set some additional requirements of the trapdoor design as follows:

1. The distribution $(\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{R})$ should be indistinguishable from uniformly random distribution;

2. the column numbers satisfy $m_1 \leq c_1 n$ and $m_2 \leq c_2 n$ for constants c_1, c_2.

The first requirement is to ensure that we can switch $\mathbf{A}$ to the *lossy model*, and the second requirement provides the constant ratio.

Now we attempt to improve the trapdoor design of [MP12] to meet these requirements. As a first attempt, we can achieve $m_2 = c_2 n$ by setting the base b of $\mathbf{G}$ as $q^{\frac{1}{c_2}}$. Then it remains to show that $\bar{\mathbf{A}}\mathbf{R}$ is uniformly at random under the parameter constraint of $m_1 = c_1 n$. As a possible way, one may consider to prove that $\bar{\mathbf{A}}\mathbf{R}$ is random by leftover hash lemma provided $\mathbf{R}$ has sufficient entropy. This approach, however, leads to a large norm of $\mathbf{R}$. This is very disadvantageous for the efficiency of our construction, especially, affects the homomorphic evaluation in the subsequent applications. A more suitable approach seems to be achieving the pseudorandomness of $\bar{\mathbf{A}}\mathbf{R}$, i,e., establish the randomness of $\bar{\mathbf{A}}\mathbf{R}$ from standard assumptions from lattices such as LWE (or a variant of LWE).

Distinguishing the distribution $(\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{R})$ from the uniform distribution is called *Knapsack Problem* [MM11, MS23]. Micciancio and Suhl [MS23] presented a mapping from the LWE instances $([\mathbf{A} \mid \mathbf{I}_m], [\mathbf{A} \mid \mathbf{I}_m] \cdot \boldsymbol{r}) \in \mathbb{Z}_q^{m \times (n+m)} \times \mathbb{Z}_q^m$ to the knapsack instances $(\bar{\mathbf{A}}, \bar{\mathbf{A}}\boldsymbol{r}') \in \mathbb{Z}_q^{m \times (n+m)} \times \mathbb{Z}_q^m$ where $\mathbf{A}$ and $\bar{\mathbf{A}}$ follow uniform distributions, and $\boldsymbol{r}$ and $\boldsymbol{r}'$ follows the same distribution over $\mathbb{Z}_q^m$. Thus with such transformation, we can build the hardness of decision knapsack problem over the hardness of LWE in Hermite normal form [ACPS09].

However, there is a gap in their proof [MS23, Lemma 20, Lemma 21]: they stated that the probability that for a uniformly random matrix from $\mathbb{Z}_q^{m \times (m+n)}$, there exists m columns that form an invertible matrix in $\mathbb{Z}_q^{m \times m}$, is at least $1 - 2^{-n+1}$. We notice that they confused the conception of existence of an invertible submatrix from $\bar{\mathbf{A}}$'s columns with the conception of non-singularity (the columns of $\bar{\mathbf{A}}$ generate $\mathbb{Z}_q$) for general modulus q. Furthermore, to the best of our knowledge, the best estimation of such probability is from Brakerski, et al. [BLP+13, Claim 2.13], which requires $n \geq 4m$ to guarantee the existence of a sub-invertible matrix from $\mathbb{Z}_q^{m \times (m+n)}$ overwhelmingly. This requirement will significantly affect the compactness of our LTF, ABM, and SO-CCA PKE scheme. Besides, the bound $n \geq 4m$ will also set constraints on the efficiency and compactness of the threshold public-key encryption (ThPKE) scheme [MS23], since the number of samples m cannot exceed a quarter of the secret dimension n in the LWE setting, which cannot support the security of their ThPKE scheme requirement $m = n$.

We give a more fine-grained and asymptotically tightest analysis of the following probability:

$$P_{m,n,q} = \Pr_{\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{m \times (m+n)}} [\exists\ m \text{ columns in } \bar{\mathbf{A}} \text{ that form an invertible matrix in } \mathbb{Z}_q^{m \times m}]$$

In Theorem 5.2, we show that for $n = t_1 + t_2 \ln\ln q$ and any modulus q, the probability is at least $1 - 2^{-(t_1+1)} - e^{-t_2/4}$, which will be $1 - \mathsf{negl}(\lambda)$ if $t_1, t_2 = \omega(\log\lambda)$ asymptotically. The estimation of the probability $P_{m,n,q}$ is divided into two steps. We seperate $m + t_1 + t_2 \ln\ln q$ vectors into two sets, where one is comprised of $m + t_1$ vectors and the other one contains $t_2 \ln\ln q$ vectors. We first use some novel combinatorial methods to prove that there exists $m - 1$ linearly independent vectors in the former $m + t_1$ vectors with probability at least $P_{m-1,m+t_1,2} \geq 1 - 2^{-(t_1+1)}$. Next, we use a theorem from number theory [Rib89] to obtain an estimation of the probability of successfully picking a final uniform vector from $\mathbb{Z}_q^n$ conditioned on the existence of $m - 1$ linearly independent vectors, and then apply the probability amplification strategy to show that there exists a valid vector in the second set except with probability $e^{-t_2/4}$.

It is worth mentioning that: (1) We also show that the constraint $n = \omega(\log\lambda) \cdot \ln\ln q$ achieves the asymptotic tightness for general modulus q (refer to Remark 5.5 for details), and we can further improve the bound to $n \geq \omega(\log\lambda)$ for certain q with constant number of prime factors; (2) $P_{m,n,q}$ is a very common and useful

probability applied in many previous works [ACPS09, BLP+13, BD20a, MS23]. Our new fine-grained analysis can reduce their security loss and improve the modulus and dimension parameters of their reductions and applications (refer more details to Remark 5.6 and 5.7); (3) there is a brief analysis of invertibility of random matrices in [BD20a], which also considers the case of composite modulus q and claims to achieve better compactness. However, their analysis is not accurate. The main flaw of their analysis is misusing CRT and union bound to calculate the probability of invertibility of a random matrix (refer more details to Remark 5.8). (4) Our technique can also be adapted to the ring-case, i.e. computing the probability of the existence of an invertible matrix in the columns of $R_p^{k\times(k+\ell)}$ since R_p is not a field but a module and behaves more like $\mathbb{Z}_q$ when q is not a prime (refers to Remark 5.9).

In a word, our new analysis achieve almost compact parameters, and should have more applications of compactness.

1.2.3 RD-based Noise Flooding for Matrix-Vector Multiplication

Unlike the reduction from (M)LWE to Entropic (M)LWR, we cannot apply the information theory method to analyse the security of decision Entropic RLWR, since the entropic secret has insufficient entropy for randomness extraction. Alternatively, our reduction follows the search-to-decision reduction framework of RLWR [LW20]. To start with, we recap the search-to-decision reduction route in [LW20]. Specifically, our reduction path can be summarized as follow.

$$\begin{aligned}\mathsf{ent\text{-}S\text{-}RLWE} &\xrightarrow{(1)} \mathsf{ent\text{-}S\text{-}RLWR} \xrightarrow{(2)} \text{(W)-}\mathfrak{p}_i\text{-RLWR} \xrightarrow{(3)} \text{(W)-D-RLWR}^i \\ &\xrightarrow{(4)} \text{(A)-D-RLWR}^i \xrightarrow{(5)} \mathsf{ent\text{-}D\text{-}RLWR}.\end{aligned}$$

We note that (1),(2),(3),(5) can be derived by similar techniques used in the work [LW20]. Thus in this part, we just overview the most interesting part (4).

Step (4) can be treated as the re-randomization of a fixed secret s in the support of initial secret domain. For the case of RLWR with polynomial modulus, one can not achieve this process by directly adding random (or Gaussian) secrets to the target sample $\lfloor a\cdot s\rceil$, due to the fact that homomorphic addition property does not hold for the rounding function. The only approach [BGM+16, LW20] is to multiply the fixed secret by a random invertible element r: transform the instance $(a, \lfloor a\cdot s\rceil)$ to $(a\cdot r, \lfloor ar\cdot r^{-1}s\rceil)$. Hence, the target here is to determine an independent distribution that somehow polynomially relates to the distribution of $r^{-1}\cdot s$. Motivated by this, we hope to use the Renyi divergence (RD) to bound these two distributions. However, there exists a technical shortcoming that almost all RD-based analyses are used to deal with the addition case.

To circumvent the this obstacle, we show a new bound of RD between another Gaussian and the product of a bounded ring element and a Gaussian. In light of that the multiplication of ring elements can be regarded as a special type of matrix-vector multiplication. Our new bound can also be served as a technique improvement of RD-based noise flooding for matrix-vector multiplication. Technically, our goal is to bound the RD of D_β^n and $\mathsf{Rot}(s)\cdot D_\alpha^n$ for a fixed $s\in R_q$. Since the distribution $\mathsf{Rot}(s)\cdot D_\alpha^n$ is exactly the same as $D_{\alpha\mathsf{Rot}(s)}$, we first do a more general computation for two continuous multivariate n-dimensional Gaussian distributions $D_{\mathbf{S}_1}$ and $D_{\mathbf{S}_2}$ with parameter matrix $\mathbf{S}_1$ and $\mathbf{S}_2$. We find that if $2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top$ is positive definite, $\mathsf{RD}_2(D_{\mathcal{S}_1}, \mathcal{D}_{\mathcal{S}_2}) = \det^2(\mathbf{S}_2)/|\det\mathbf{S}_1|\cdot\sqrt{\det(2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top)}$. In our case, $\mathbf{S}_1=\beta\mathbf{I}_n$ and $\mathbf{S}_2=\alpha\mathsf{Rot}(s)$, so $\det(\mathbf{S}_1)=\beta^n$, then our target is an appropriate lower bound for

$$\frac{\det^2(\alpha\mathsf{Rot}(s))}{\det(2\alpha^2\mathsf{Rot}(s)\mathsf{Rot}(s)^\top-\beta^2\mathbf{I}_n)}.$$

For the case that $K = \mathbb{Q}[X]/(X^n+1)$ is a cyclotomic field with n a power of 2, we can enjoy a nice structure of the rotation matrix $\mathsf{Rot}(s)$ which is exactly an anti-circulant matrix. Let s_i be the i-th coefficient of s under the basis $\mathbf{B}$ for $i = 0, \cdots, n-1$ and $\{\lambda_i \in C\}_i$ be n eigenvalues of $\mathsf{Rot}(s)$ (may exist same values). Denote $\mathbf{S} = \mathsf{Rot}(s)$. We notice the following several interesting points:

- For anti-circulant matrix $\mathbf{S}$, every *Gershgorin circle* becomes the disk with center s_0 and radius $\sum_{i\neq 0}|s_i|$, so we can bound every eigenvalue with the same inequality $|s_0| - \sum_{i\neq 0}|s_i| \leq |\lambda_i| \leq \sum_i |s_i|$.
- Anti-circulant matrix $\mathbf{S}$ is also a normal matrix, indicating that the eigenvalues of $2\alpha^2\mathbf{S}\mathbf{S}^\top - \beta^2\mathbf{I}_n$ are exactly $2\alpha^2|\lambda_i|^2 - \beta^2$. We can compute the RD as:

$$\mathsf{RD}_2(D_\beta^n \| D_{\alpha\mathbf{S}}) = \frac{\alpha^n}{\beta^n} \cdot \prod_{i=0}^{n-1} \frac{|\lambda_i|^2}{\sqrt{2|\lambda_i|^2 - (\beta/\alpha)^2}}.$$

Based on these points, we can finally obtain an upper bound of this product by our first observation.

2 Preliminaries

2.1 Notations

Let λ denote the security parameter. For an integer n, let $[n]$ denote the set $\{1, ..., n\}$. We use bold lowercase letters (e.g. $\boldsymbol{a}$) to denote vectors and bold capital letters (e.g. $\mathbf{A}$) to denote matrices. For a positive integer $q \geq 2$, let $\mathbb{Z}_q$ be the ring of integers modulo q. For a distribution on a set X, we write $x \xleftarrow{\$} X$ to denote the operation of sampling a random x according to X. For distributions X, Y, we let $\mathsf{SD}(X, Y)$ denote their statistical distance. We write $X \overset{s}{\approx} Y$ or $X \overset{c}{\approx} Y$ to denote statistical closeness or computational indistinguishability, respectively. We use $\mathsf{negl}(\lambda)$ to denote the set of all negligible functions $\mu(\lambda) = \lambda^{-\omega(1)}$. We define a distribution χ over $\mathbb{Z}$ to be β-bounded if $\mathsf{Supp}(\chi) \subseteq [-\beta, \beta]$.

We use $\left(\mathbb{Z}_q^n\right)^*$ to denote the set of vectors in $\mathbb{Z}_q^n$ which are not zero-divisors, i.e., $\left(\mathbb{Z}_q^n\right)^* = \{\boldsymbol{x} \in \mathbb{Z}_q^n : \gcd(x_1, \ldots, x_n, q) = 1\}$. The ratio of $\left|\left(\mathbb{Z}_q^n\right)^*\right|$ in $\left|\mathbb{Z}_q^n\right|$ has the lower bound $\frac{|(\mathbb{Z}_q^n)^*|}{|\mathbb{Z}_q^n|} \geq 1 - 2^{-n+1}$.

We need the following bound on the sum of total power of prime.

Lemma 2.1. *Let $t \geq 2$ be a positive integer and $\{p_i\}_{i\geq 1}$ be all different sequenced primes. We have $\sum_{i=1}^{\infty} p_i^{-t} < 2^{-(t-1)}$.*

Proof. In the case $t \geq 3$,

$$\begin{aligned}
\sum_{i=1}^{\infty} p_i^{-t} &< 2^{-t} + 3^{-t} + \sum_{j=2}^{\infty} (2j)^{-t} = 2^{-t} \cdot \left(1 + \left(\frac{3}{2}\right)^{-t} + \sum_{j=2}^{\infty} j^{-t}\right) \\
&= 2^{-t} \cdot \left(1 + \left(\frac{3}{2}\right)^{-t} + \int_1^{\infty} x^{-t} dx\right) \\
&= 2^{-t} \cdot \left(1 + \left(\frac{3}{2}\right)^{-t} + \frac{1}{t-1}\right) < 2^{-(t-1)}.
\end{aligned}$$

For the case $t = 2$,

$$\begin{aligned}\sum_{i=1}^{\infty} p_i^{-2} &< \sum_{i=1}^{\infty} i^{-2} - 1 - \sum_{i=2}^{\infty} (2i)^{-2} \\ &= \sum_{i=1}^{\infty} i^{-2} - 1 - \frac{1}{4}\left(\sum_{i=1}^{\infty} i^{-2} - 1\right) \\ &= \frac{3}{4}\left(\sum_{i=1}^{\infty} i^{-2} - 1\right) = \frac{3}{4}\left(\frac{\pi^2}{6} - 1\right) < 2^{-1}.\end{aligned}$$

□

2.2 Rounding Functions

For any integer modulus $q \geq 2$, we use the "*rounding*" function defined in [BPR12] – for $q \geq p \geq 2$, let $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ be the function as $\lfloor x \rceil_{q,p} = \lfloor (p/q) \cdot \bar{x} \rceil \bmod p$, where $\bar{x} \in \mathbb{Z}$ is any integer congruent to x mod q. We write $\lfloor \cdot \rceil_p$ for short.

Definition 2.2. *For integers $q \geq p \geq 2$ and any rational numbers $0 \leq \nu < 1$ and $\tau > 0$, we define the following set:*

$$\mathsf{border}_{p,q,\nu}(\tau) \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_q + \nu : \exists\, y \in \mathbb{Q}, |y| \leq \tau, \lfloor x \rceil_p \neq \lfloor x + y \rceil_p\}.$$

For any rational number $0 \leq \nu < 1$, the distribution $U(\mathbb{Z}_q) + \nu$ is defined by sampling a uniformly random variable u in $\mathbb{Z}_q$ and outputting $u + \nu$. Similarly, we denote $\mathbb{Z} + \nu$ as the set $\{y : y = x + \nu, x \in \mathbb{Z}\}$.

Lemma 2.3. *We have $\left|\mathsf{border}_{p,q,\nu}(\tau)\right| \leq 2\tau p$, and thus $\mathsf{Pr}_{x \sim U(\mathbb{Z}_q)+\nu}[x \in \mathsf{border}_{p,q,\nu}(\tau)] \leq \frac{2\tau p}{q}$.*

Proof. Let $S = \bigcup_{i \in \{0,\cdots,p-1\}} ((i + \frac{1}{2})\frac{q}{p} - \tau, (i + \frac{1}{2})\frac{q}{p} + \tau]$ be a subset over the reals. It's easy to see that $\mathsf{border}_{p,q,\nu}(\tau) = (\mathbb{Z} + \nu) \cap S$ and therefore $|\mathsf{border}_{p,q,\nu}(\tau)| \leq 2\tau p$. The lemma follows. □

Rounding of Ring Elements. We recap the definition of rounding over ring.

Definition 2.4 (Rounding according to basis [LW20])**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field with degree n, and $\mathcal{I}$ be a fractional ideal over K with a $\mathbb{Z}$-basis $\mathbf{B} = \{b_1, \cdots, b_n\}$. Then for any integers $q \geq p \geq 2$, we define the rounding function (with respect to basis $\mathbf{B}$) $\lfloor \cdot \rceil_{\mathbf{B},p} : \mathcal{I}_q \to \mathcal{I}_p$ as*

$$\lfloor a \rceil_{\mathbf{B},p} = \lfloor x_1 \rceil_p b_1 + \cdots + \lfloor x_n \rceil_p b_n \mod p\mathcal{I},$$

where $\mathcal{I}_q$ (similarly $\mathcal{I}_p$) is the quotient groups $\mathcal{I}/q\mathcal{I}$, and $a = x_1 b_1 + \cdots + x_n b_n \in \mathcal{I}_q, x_1, \cdots, x_n \in \mathbb{Z}_q$. The rounding function for $\mathbb{Z}_q \to \mathbb{Z}_p$, i.e., $\lfloor \cdot \rceil_p$, is the same as described above.

2.3 Rényi Divergence and Min-Entropy

The *Rényi divergence* (RD) [Rén61, BLL+15] defines a measure of distribution closeness. This notion has many useful application in cryptography – for example, Bai et al. [BLL+15] used RD as a powerful tool to analyze hardness and security of certain lattice-based crypto systems. The definition is as follows:

Definition 2.5 (Rényi divergence)**.** *Let $\mathcal{P},\mathcal{Q}$ be two discrete distributions s.t. Supp($\mathcal{P}$) $\subseteq$ Supp($\mathcal{Q}$). For $a \in (1,+\infty)$, the Rényi divergence of order a is defined as*

$$\mathsf{RD}_a(\mathcal{P}\|\mathcal{Q}) = \left(\sum_{x \in Supp(\mathcal{P})} (\mathcal{P}(x)^a / \mathcal{Q}(x)^{a-1}) \right)^{\frac{1}{a-1}}.$$

Specifically, the Rényi divergence of order $+\infty$ is given by

$$\mathsf{RD}_\infty(\mathcal{P}\|\mathcal{Q}) = \max_{x \in Supp(\mathcal{P})} (\mathcal{P}(x)/\mathcal{Q}(x)).$$

If $\mathcal{P},\mathcal{Q}$ are two continuous distributions s.t. Supp($\mathcal{P}$) $\subseteq$ Supp($\mathcal{Q}$). For $a \in (1,+\infty)$, an analogous version for Rényi divergence of order a is defined as

$$\mathsf{RD}_\alpha(\mathcal{P}\|\mathcal{Q}) = \left(\int_{x \in Supp(\mathcal{P})} \mathcal{P}(x)^\alpha \mathcal{Q}(x)^{1-\alpha} dx \right)^{\frac{1}{\alpha-1}}$$

The Rényi divergence admits the following properties.

Lemma 2.6 ([BLL+15])**.** *For tow distributions $\mathcal{P},\mathcal{Q}$ and two families of distributions $(\mathcal{P}_i)_i, (\mathcal{Q}_i)_i$, the Rényi divergence verifies the following properties:*

- ***Data Processing Inequality.*** *For any function f, $\mathsf{RD}_a(f(\mathcal{P})\|f(\mathcal{Q})) \leq \mathsf{RD}_a(\mathcal{P}\|\mathcal{Q})$.*
- ***Multiplicativity.*** *$\mathsf{RD}_a(\prod_i \mathcal{P}_i \| \prod_i \mathcal{Q}_i) = \prod_i \mathsf{RD}_a(\mathcal{P}_i\|\mathcal{Q}_i)$, if $\{\mathcal{P}_i\}_i$ are mutually independent and $\{\mathcal{Q}_i\}_i$ are mutually independent.*
- ***Probability preservation.*** *For any event $E \subseteq Supp(\mathcal{Q})$ and $a \in (1,+\infty)$,*

$$\mathcal{Q}(E) \geq \frac{\mathcal{P}(E)^{a/(a-1)}}{\mathsf{RD}_a(\mathcal{P}\|\mathcal{Q})}, \qquad \mathcal{Q}(E) \geq \frac{\mathcal{P}(E)}{\mathsf{RD}_\infty(\mathcal{P}\|\mathcal{Q})}.$$

The *min-entropy* of a random variable X is $H_\infty(X) \stackrel{\text{def}}{=} -\log(\max_x \Pr[X = x])$, which measures the maximal probability of elements in X. The *conditional min-entropy* of X conditioned on Z is $H_\infty(X \mid Z) \stackrel{\text{def}}{=} -\log(\mathbb{E}_{z \leftarrow Z}[\max_x \Pr[X = x \mid Z = z]])$, which measures the best guess for X given a correlated random variable Z.

Definition 2.7 (Smooth Entropy, Definition 2.3 in [AKPW13])**.** *The ε-smooth min-entropy of a random variable X is at least e, denoted by $H^\varepsilon_\infty(X) \geq e$, if there exists another variable X' such that $\Delta(X,X') \leq \varepsilon$ and $H_\infty(X') \geq e$. If $\varepsilon = \mathsf{negl}(\lambda)$, we can omit ε and write $H^{\mathsf{smooth}}_\infty$ for the smooth min-entropy. Similarly, the ε-smooth conditional min-entropy of X given Y is at least e, denoted by $H^\varepsilon_\infty(X \mid Y) \geq e$, if there exists other variables $(X'|Y')$ such that $\Delta((X,Y);(X',Y')) \leq \varepsilon$ and $H_\infty(X' \mid Y') \geq e$.*

Lemma 2.8 (Lemma 2.4 in [AKPW13])**.** *Let X,Y,Z be correlated random variables and $\mathcal{Z}$ be some set such that $\Pr[\ Z \in \mathcal{Z}\ ] \geq 1-\varepsilon$ and $|\mathcal{Z}| \leq 2^\lambda$. Then, for any $\varepsilon' > 0$, $H^{\varepsilon+\varepsilon'}_\infty(X \mid Y,Z) \geq H^{\varepsilon'}_\infty(X \mid Y) - \lambda$.*

2.4 Lattices

A lattice $\Lambda \subset \mathbb{R}^n$ is the set of all integer linear combinations of t linearly independent basis vectors $\mathbf{B} = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_t) \in \mathbb{R}^{n \times t}$, i.e., $\Lambda = \mathbf{B} \cdot \mathbb{Z}^t$. We call t the rank of the lattice. If $t = n$, we call Λ a full-rank lattice.

A lattice is a discrete additive subgroup of $\mathbf{R}^n$. For sub-lattice $\Lambda' \subseteq \Lambda$, the quotient group Λ/Λ' is well-defined as the additive group of distinct cosets $\boldsymbol{v} + \Lambda'$ for $\boldsymbol{v} \in \Lambda$. The vector $\boldsymbol{v}$ is called the coset representative of $\boldsymbol{v} + \Lambda'$.

The length of the shortest non-zero vector in L_p norm of a lattice Λ is denoted as $\lambda_1^p(\Lambda) := \min_{\boldsymbol{x} \in \Lambda/\{0\}} \|\boldsymbol{x}\|_p$. The dual lattice of Λ is defined as $\Lambda^\vee := \{\boldsymbol{y} \in \mathsf{span}(\Lambda) \mid \langle \boldsymbol{y}, \Lambda \rangle \subseteq \mathbb{Z}\}$, i.e., the set of all vectors that have integer inner product with all lattice vectors in Λ. It is easy to see that $(\Lambda^\vee)^\vee = \Lambda$. For a lattice Λ and its one set of basis $\mathbf{B} \in \mathbb{R}^{n \times n}$, the set $\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot [-1/2, 1/2)^n$ is called the fundamental parallelepiped defined by the basis. For a point $\boldsymbol{c} \in \mathbb{R}^n$, we write $\boldsymbol{c}' := \boldsymbol{c} \bmod \mathcal{P}(\mathbf{B})$ for the unique element $\boldsymbol{c}'$ s.t. $\boldsymbol{c} = \boldsymbol{c}' + \boldsymbol{x}$ for some lattice point $\boldsymbol{x} \in \Lambda$. Equivalently, if $\boldsymbol{c} = \mathbf{B} \cdot \boldsymbol{v}$ for $\boldsymbol{v} \in \mathbb{R}^n$, then $\boldsymbol{c} \bmod \mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot (\boldsymbol{x} - \lfloor \boldsymbol{x} \rceil)$.

Let $\mathbf{A} \in \mathbb{Z}^{n \times m}$ for some positive integers n, m and we define two lattices given by $\mathbf{A}$,

$$\begin{aligned} \Lambda(\mathbf{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \mathbf{A}^\top \cdot \boldsymbol{s} \text{ for some } \boldsymbol{s} \in \mathbb{Z}^n\} \\ \Lambda^\perp(\mathbf{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \boldsymbol{e} = 0\}, \end{aligned}$$

and two q-ary lattices given by $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some positive modulus q:

$$\begin{aligned} \Lambda_q(\mathbf{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \mathbf{A}^\top \cdot \boldsymbol{s} \mod q \text{ for some } \boldsymbol{s} \in \mathbb{Z}_q^n\} \\ \Lambda_q^\perp(\mathbf{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \boldsymbol{e} = 0 \mod q\}. \end{aligned}$$

2.5 Gaussians

Positive Definite. We say that a square matrix $\Sigma \in \mathbb{R}^{n \times n}$, iff for every $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{x} \neq \mathbf{0}$, it holds that $\mathbf{x}^\top \Sigma \mathbf{x} > 0$, abbreviated by $\Sigma > 0$. For any $\Sigma > 0$, there exists a unique matrix $\sqrt{\Sigma} > 0$ such that $\sqrt{\Sigma}\sqrt{\Sigma}^\top = \Sigma$.

Continuous Gaussians. For a positive definite matrix Σ, the multivariate n-dimensional Gaussian function $\rho_\sigma : \mathbb{R}^n \to \mathbb{R}$ with matrix parameter Σ centered at $\mathbf{c} \in \mathbb{R}^n$ is defined as

$$\rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x}) := \exp(-\pi(\mathbf{x}-\mathbf{c})^\top \Sigma^{-1}(\mathbf{x}-\mathbf{c})) = \exp\left(-\pi \left\| \sqrt{\Sigma}^{-1}(\mathbf{x}-\mathbf{c}) \right\|^2\right).$$

The continuous Gaussian distribution $D_{\sqrt{\Sigma}}$ of matrix parameter $\sqrt{\Sigma}$ over $\mathbb{R}^n$ is defined as the probability function proportional to $\rho_{\sqrt{\Sigma}}$, since $\int_{\mathbb{R}^n} \rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{y}) d\mathbf{y} = \sqrt{\det \Sigma}$ for all positive definite Σ and center $\mathbf{c} \in \mathbb{R}^n$, we have

$$D_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x}) := \frac{\rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x})}{\sqrt{\det \Sigma}}.$$

For convenience, we will omit $\mathbf{c}$ if $\mathbf{c} = \mathbf{0}$. We will write $D_{\sigma,\mathbf{c}}$ in short if $\Sigma = \sigma^2 \mathbf{I}$ for some Gaussian parameter $\sigma > 0$.

Discrete Gaussians. For a positive definite matrix Σ, we represent the discrete Gaussian distribution with matrix parameter $\sqrt{\Sigma}$ over some n-dimensional lattice Λ and coset vector $\mathbf{u} \in \mathbb{R}^n$ as $D_{\Lambda+\mathbf{u},\sqrt{\Sigma}}$ with mass function

$$D_{\Lambda+\mathbf{u},\sqrt{\Sigma}}(\mathbf{x}) = \frac{\rho_{\sqrt{\Sigma}}(\mathbf{x})}{\rho_{\sqrt{\Sigma}}(\Lambda+\mathbf{u})}, \text{for} \mathbf{x} \in \Lambda.$$

2.6 Algebraic Number Theory Background

Algebraic number theory is the study of number fields. Below we present the requisite concepts and notations used in this work. More backgrounds and complete proofs can be found in any introductory book on the subject, e.g., [Ste04, Cona].

2.6.1 The Space H

When working with number fields and algebraic number theory, it is convenient to work with a certain linear subspace $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ for some integers $s_1, s_2 > 0$ such that $s_1 + 2s_2 = n$, defined as

$$H = \{(x_1, \cdots x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} | x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \forall j \in [s_2]\}.$$

As described in the work [LPR10], we can equip H with norms, which would naturally define norms of elements in a number field or ideal lattice via an embedding that maps field elements into H. We will present more details next.

It is not hard to verify that H equipped with the inner product induced by $\mathbb{C}^n$, is isomorphic to $\mathbb{R}^n$ as an inner product space. We denote $\Theta : H \to \mathbb{R}^n$ as this isomorphism.

We can equip H with the ℓ_2 and ℓ_∞ norms induced on it from $\mathbb{C}^n$. Namely, for $\boldsymbol{x} \in H$ we have $\|\boldsymbol{x}\|_2 = \sum_i (|x_i|^2)^{1/2} = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ and $\|\boldsymbol{x}\|_\infty = \max_i |x_i|$. ℓ_p norms can be defined similarly.

2.6.2 Number Fields and Their Geometry

A *number field* can be defined as a field extension $K = \mathbb{Q}(\alpha)$ obtained by adjoining an abstract element α to the field of rationals, where α satisfies the relation $f(\alpha) = 0$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$, called *minimal polynomial* of α, which is monic without loss of generality. The *degree* n of the number field is the degree of f.

A number field $K = \mathbb{Q}(\alpha)$ of degree n has exactly n field embeddings (injective homomorphisms) $\sigma_i : K \to \mathbb{C}$. Concretely, these embeddings map α to each of the complex roots of its minimal polynomial f. An embedding whose images lies in $\mathbb{R}$ is said to be *real*, or otherwise it is *complex*. Because roots of f come in conjugate pairs, so do the complex embeddings. The number of real embeddings is denoted as s_1 and the number of pairs of complex embeddings is denoted as s_2, satisfying $n = s_1 + 2s_2$ with σ_i for $1 < i < s_1$ being the real embeddings and $\sigma_{s_1+s_2+i} = \overline{\sigma_{s_1+i}}$ for $1 \le i \le s_2$ being the conjugate pairs of complex embeddings.

The *canonical embedding* $\sigma : K \leftarrow \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ is then defined as $\sigma(x) = (\sigma_1(x), \cdots \sigma_n(x))$. Note that σ is a ring homomorphism from K to H, where multiplication and addition in H are both component-wise.

By identifying elements of K and their canonical embeddings on H, we can define the norms on K. For any $x \in K$ and any $p \in [1, \infty]$, the ℓ_p norm of x is simply $\|x\|_p = \|\sigma(x)\|_p$. Then we have that $\|xy\|_p \le \|x\|_\infty \cdot \|y\|_p \le \|x\|_p \cdot \|y\|_p$, for any $x, y \in K$ and $p \in [1, \infty]$.

The canonical embedding also allows us to view Gaussian distribution $D_{\boldsymbol{r}}$ over H, or their discrete analogues over a lattice $\mathcal{L} \subset H$, as distributions over K. Formally, the continuous distribution $D_{\boldsymbol{r}}$ is actually over the field tensor product $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, which is isomorphic to H. Let $\bar{\Theta} : K_{\mathbb{R}} \to \mathbb{R}^n$ be the metric isomorphism from $K_{\mathbb{R}}$ to $\mathbb{R}^n$, $\bar{\Theta}$ is just the concatenation of σ and Θ.

2.6.3 Ring of Integers and Ideals

An *algebraic integer* is an algebraic number whose minimal polynomial over the rationals has integer coefficients. For a number field K, we denote its subset of algebraic integers by $R = O_K$. This set forms a ring, called the *ring of integers* of the number field. The norm of any algebraic integer is in $\mathbb{Z}$. For any modulus q and ring of integers R, we define $R_q = R/qR$ to be the quotient ring.

An (*integer*) *ideal* $\mathcal{I} \subseteq O_K$ is an additive subgroup that is closed under multiplication by R. Every ideal in O_K is the set of all $\mathbb{Z}$-linear combinations of some basis $\{b_1, \cdots, b_n\} \subset \mathcal{I}$. An ideal $\mathfrak{p} \subsetneq O_K$ is *prime* if $ab \in \mathfrak{p}$ for some $a, b \in O_K$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both). In O_K, an ideal $\mathfrak{p}$ is prime if and only if it is maximal, which implies that the quotient ring $O_K/\mathfrak{p}$ is a finite field of order $N(\mathfrak{p})$.

An ideal $\mathfrak{p} \subsetneq O_K$ is *prime* if $ab \in \mathfrak{p}$ for some $a, b \in O_K$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both). In O_K, an ideal $\mathfrak{p}$ is prime if and only if it is maximal, which implies that the quotient ring $O_K/\mathfrak{p}$ is a finite field of order $N(\mathfrak{p})$. An ideal $\mathcal{I}$ is called to *divide* ideal $\mathcal{J}$, which is written as $\mathcal{I}|\mathcal{J}$, if there exists another ideal $\mathcal{H} \in O_K$ such that $\mathcal{J} = \mathcal{H}\mathcal{I}$. Two ideal $\mathcal{I}, \mathcal{J} \subseteq O_K$ are *coprime* if $\mathcal{I} + \mathcal{J} = O_K$.

2.6.4 Ideal Lattices

Recall that an ideal $\mathcal{I}$ of O_K has a $\mathbb{Z}$-basis $\mathbf{B} = \{b_1, \cdots, b_n\}$. Therefore, under the canonical embedding σ, the ideal yields a full-rank lattice $\sigma(\mathcal{I})$ have basis $\sigma(\mathbf{B}) = \{\sigma(b_1), \cdots, \sigma(b_n)\} \subset H$. According map Θ, we further obtain a lattice $\Lambda = \bar{\Theta}(\mathcal{I}) \subseteq \mathbb{R}^n$ with basis $\bar{\mathbf{B}} = \bar{\Theta}(\mathbf{B})$. In some cases, we also consider the coefficient embedding ϕ, i.e., the ideal thus also yields a full-rank lattice $\phi(\mathcal{I})$, which has basis $\mathbf{B}$.

2.6.5 Duality

For any lattice $\mathcal{L} \subseteq K$ (i.e., for the $\mathbb{Z}$-span of any $\mathbb{Q}$-basis of K), its *dual* is defined as $\mathcal{L}^\vee = \{x \in K : \mathrm{Tr}(x\mathcal{L}) \subseteq \mathbb{Z}\}$.

Then $\mathcal{L}^\vee$ embeds as the complex conjugate of the dual lattice,i.e., $\sigma(\mathcal{L}^\vee) = \overline{\sigma(\mathcal{L})^*}$ due to the fact that $\mathrm{Tr}(xy) = \sum_i \sigma_i(x)\sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle$. It is easy to check that $(\mathcal{L}^\vee)^\vee = \mathcal{L}$, and that if $\mathcal{L}$ is a fractional ideal, then $\mathcal{L}^\vee$ is one as well.

We point out that the ring of integers $R = O_K$ is not self-dual, nor are an ideal and its inverse dual to each other. For any fractional ideal $\mathcal{I}$, its dual ideal is $\mathcal{I}^\vee = \mathcal{I}^{-1} \cdot R^\vee$. The factor $R^\vee$ is a fractional ideal whose inverse $(R^\vee)^{-1}$, called the *different ideal*, is integral and of norm $N((R^\vee)^{-1}) = \Delta_K$. The fractional ideal $R^\vee$ itself is often called the *codifferent*.

For any $\mathbb{Q}$-basis $\mathbf{B} = \{b_j\}$ of K, we denote its dual basis by $\mathbf{B}^\vee = \{b_j^\vee\}$, which is characterized by $\mathrm{Tr}(b_i \cdot b_j^\vee) = \delta_{ij}$, the Kronecker delta. It is immediate that $(B^\vee)^\vee = B$, and if $\mathbf{B}$ is a $\mathbb{Z}$-basis of some fractional ideal $\mathcal{I}$, then $\mathbf{B}^\vee$ is a $\mathbb{Z}$-basis of its dual ideal $\mathcal{I}^\vee$. If $a = \sum_j a_j \cdot b_j$ for $a_j \in \mathbb{R}$ is the unique presentation of $a \in K_\mathbb{R}$ in basis $\mathbf{B}$, then $a_j = \mathrm{Tr}(a \cdot b^\vee)$.

2.6.6 Prime Splitting and Chinese Remainder Theorem

For an integer prime $p \in \mathbb{Z}$, the factorization of the principal ideal $\langle p \rangle \subset R = O_K$ for a number field K (where $K/\mathbb{Q}$ is a field extension with degree n) is as follows.

Lemma 2.9 (Dedekind [Conb])**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field for $\alpha \in O_K$, and $F(x)$ be the minimal polynomial of α in $\mathbb{Z}[x]$. For any prime p, the ideal pO_K factors into prime ideals as $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, where $N(\mathfrak{p}_i) = p^{f_i}$ for $f_i = [O_K/\mathfrak{p}_i : \mathbb{Z}_p]$, and $n = \sum_{i=1}^g e_i f_i$.*

Moreover if p does not divide the index of $[O_K : \mathbb{Z}[\alpha]]$, then we have further structures as following. We can express $F(x) = f_1(x)^{e_1} \dots f_g(x)^{e_g} \mod p$, where each $f_i(x)$ is a monic irreducible polynomial in $\mathbb{Z}_p[x]$. There exists a bijection between $\mathfrak{p}_i$'s and $f_i(x)$'s such that $\mathfrak{p}_i = \langle p, f_i(\alpha) \rangle$, and $f_i = \deg f_i(x)$.

For each $\mathfrak{p}_i$, we have $\mathfrak{p}_i \mid pO_K$, which can be written as $\mathfrak{p}_i | \langle p \rangle$, and call $\mathfrak{p}_i$ a factor of $\langle p \rangle$. We can easily generalize Lemma 2.9 to the case of composite number as follows.

Lemma 2.10. *Let $K = \mathbb{Q}(\alpha)$ be a number field for $\alpha \in O_K$. For any composite number q with decomposition $q = \prod_i^t p_i^{x_i}$, where p_i is the prime factor of q. Then the ideal qO_K factors into prime ideals as $\langle q \rangle = \prod_i^t \mathfrak{p}_{i,1}^{e_{i,1}} \cdots \mathfrak{p}_{i,g_i}^{e_{i,g_i}}$, where $N(\mathfrak{p}_{i,j}) = p_i^{f_{i,j}}$ for $f_{i,j} = [O_K/\mathfrak{p}_{i,j} : \mathbb{Z}_{p_i}]$, and $nx_i = \sum_{j=1}^{g_i} e_{i,j} f_{i,j}$.*

If considering the case that K is a cyclotomic ring, it further enjoys the good splitting property that $e_{i,1} = \cdots = e_{i,g_i}$ and $f_{i,1} = \cdots = f_{i,g_i}$ for each $i \in [t]$.

Next we recall the Chinese Remainder Theorem (CRT) for the fraction ideal over a number field K.

Lemma 2.11 (Chinese Remainder Theorem [BBPS19]). *Let $\mathcal{I}$ be a fractional ideal over K, and let $\mathfrak{p}_i$ be pairwise coprime ideals in $R = \mathcal{O}_K$, then natural ring homomorphism is an isomorphism: $\mathcal{I}/\left(\prod_i \mathfrak{p}_i\right)\mathcal{I} \to \bigoplus_i (\mathcal{I}/\mathfrak{p}_i\mathcal{I})$.*

As a corollary of Chinese Remainder Theorem above, the following lemma states the equivalence of prime ideal factors of qR and $qR^\vee$ under isomorphism.

Lemma 2.12 (Lemma 2.35 of [BBPS19]). *Let $\mathcal{I}, \mathcal{J}$ be integral ideals in an order $\mathcal{O}$ and let $\mathcal{M}$ be a fractional $\mathcal{O}$-ideal. Assume that $\mathcal{I}$ is invertible. Given the associated primes of $\mathcal{J}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$, and an element $t \in \mathcal{I} \setminus \bigcup_{j=1}^{k} \mathfrak{p}_j\mathcal{I}$ the map*

$$\begin{aligned} \theta_t : \mathcal{M}/\mathcal{J}\mathcal{M} &\to \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{J}\mathcal{M} \\ x &\mapsto t \cdot x \end{aligned}$$

induces an isomorphism of $\mathcal{O}$-modules. Moreover, θ_t is efficiently inverted given $\mathcal{I}, \mathcal{J}, \mathcal{M}$ and t, and t can be computed given $\mathcal{I}$ and $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$.

In particular, let $\mathcal{I} = (R^\vee)^{-1}, \mathcal{J} = qR, \mathcal{M} = R^\vee$, then $R/qR \cong R^\vee/qR^\vee$.

Finally, as an application of prime splitting and CRT, we have the following lemma.

Lemma 2.13 (Generalization of Lemma 3.5 in [SS13]). *Let $R = \mathbb{Z}[X]/(X^n + 1)$ with $n \geq 8$ a power of 2, $p > n$ be a prime such that $\langle p \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, $q = p^t$ be a (constant) power of p. $\sigma \geq \sqrt{n \ln(2n(1+n^2))/\pi} \cdot p^{1/g}$. Let $B = \{1, X, \cdots, X^{N-1}\}$. Then it holds that*

$$\mathsf{Pr}_{x \leftarrow D_{R,\sigma}^{\mathsf{Coeff}(\mathbf{B})}}\left[x \in (R_q)^*\right] \geq 1 - g(1/p + 2/n^2) \geq 1 - n(1/p + 2/n^2).$$

2.7 General-LWE Problem and HNFLWE Problem

We now provide the definition of the LWE problem, including four versions, e.g. plain LWE, (non-dual) Ring-LWE , Module-LWE and HNFLWE. In this paper, we consider the "non-dual" form of RLWE defined in [Pei16b], and various LWE problems with discrete error distribution for convenience of our analyses and applications.

Definition 2.14 (GLWE distribution). *Let R be a sub-ring of a number field K, $q \geq 2$, $k \geq 1$ be positive integers and χ be an discrete error distribution over R_q. For $\boldsymbol{s} \in R_q^k$, a sample from the GLWE distribution $A_{\boldsymbol{s},q,\chi}^{R,k}$ over R_q^{k+1} is generated by choosing $\boldsymbol{a} \xleftarrow{\$} R_q^k$ uniformly at random and error $e \leftarrow \chi$, outputting $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$.*

Definition 2.15 (GLWE problem, decision). *The decision problem $\mathsf{D\text{-}GLWE}_{m,q,\chi}^{R,k}$ is to distinguish between m samples from $A_{\boldsymbol{s},q,\chi}^{R,k}$ where $\boldsymbol{s} \xleftarrow{\$} R_q^k$, and m samples from $U(R_q^{k+1})$.*

Definition 2.16 (GLWE problem, search). *The search problem $\mathsf{S\text{-}GLWE}_{m,q,\chi}^{R,k}$ is given m samples from $A_{\boldsymbol{s},q,\chi}^{R,k}$ for $\boldsymbol{s} \xleftarrow{\$} R_q^k$, find $\boldsymbol{s}$.*

We can capture several LWE variants by choosing the appropriate ring R and dimension k. Let $R = \mathbb{Z}$ and $k > 1$, the problem becomes the plain LWE problem [Reg05]. Alternatively, if we choose $R = O_K$ and $k = 1$, we obtain the (non-dual) RLWE problem [Pei16b]. Furthermore, by taking $R = O_K$ and $k > 1$, we get Module LWE [LS15].

In our compact gadget trapdoor scheme, we need to prove the pseudorandomness of public matrix $\mathbf{A}$ based on the plain HNFLWE problem where each entry of secret $\boldsymbol{s}$ follows the same distribution as error χ. We only introduce the plain version of the decision HNFLWE problem (choose $R = \mathbb{Z}$ and $k = n$).

Definition 2.17 (HNFLWE problem [ACPS09])**.** *The decision problem* $\mathsf{HNFLWE}_{n,m,q,\chi}$ *is to distinguish between* m *samples from* $A^{\mathbb{Z},n}_{s,q,\chi}$ *where* $\boldsymbol{s} \leftarrow \chi^k$*, and* m *samples from* $U(R_q^{k+1})$.

For the hardness of these LWE problems, the works of [Reg05, Pei09, ACPS09, LPR10, LS15, PP19] show these LWE problems are as hard as (quantum or classical) various lattice problems under various parameter regimes. We summarize the hardness of all versions of LWE in Appendix 2.9.

2.8 General-LWR Problem

The learning with rounding problem in some sense, can be seen as a de-randomized version of the LWE problem. In this paper, we consider three types LWR problems, e.g., LWR over $\mathbb{Z}^n$, (non-dual) RLWR and Module-LWR. To simplify our presentation, we define a "General Learning with Errors (GLWR)" problem, which captures the three types LWR.

Definition 2.18 (GLWR distribution)**.** *Let* R *be a sub-ring of a number field* K*,* $q \geq p \geq 2$*,* $k \geq 1$ *be positive integers, and* $\mathbf{B}$ *be a basis of* R*. For* $\boldsymbol{s} \in (R_q)^k$*, a sample from the* GLWR *distribution* $L^k_{s,q,p}(R, \mathbf{B})$ *over* $(R_q)^k \times R_p$ *is generated by choosing* $\boldsymbol{a} \leftarrow (R_q)^k$ *uniformly at random, outputting* $(\boldsymbol{a}, b = \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_{\mathbf{B},p})$.

Definition 2.19 (GLWR problem, decision)**.** *The decision problem* $D\text{-}\mathsf{GLWR}^k_{\mathbf{B},q,p,\ell,\psi}$ *is to distinguish between* ℓ *samples from* $L^k_{s,q,p}(R, \mathbf{B})$ *where* $\boldsymbol{s} \leftarrow \psi \subseteq R_q^k$*, and* ℓ *samples from* $U((R_q)^k \times R_p)$.

Definition 2.20 (GLWR problem, search)**.** *The search problem* $S\text{-}\mathsf{GLWR}^k_{\mathbf{B},q,p,\ell,\psi}$ *is given* ℓ *samples from* $L^k_{s,q,p}(R, \mathbf{B})$ *for* $\boldsymbol{s} \leftarrow \psi \subseteq R_q^k$*, find* $\boldsymbol{s}$.

For simplicity of notation, we omit the subscript ψ for the uniform distribution for the above two definitions. Below the computational problems are all *average-case*, where distinguishability/solvability is referred to the case when the secret $\boldsymbol{s}$ comes from some distribution. We also define their *worst-case* variants by adding (W), i.e., (W)-GLWR, where solvability means finding solutions for any $\boldsymbol{s}$ in the support of ψ, i.e., for any $\boldsymbol{s} \in \mathsf{Supp}(\psi)$.

The definitions above captures a few LWR variants. For example, let $R = \mathbb{Z}, \mathbf{B} = 1$ and $k > 1$, we obtain the plain LWR problem defined in [BPR12]. Alternatively, by taking $R = O_K$ and $k = 1$, we get the "primal" form of RLWR over O_K. Furthermore, if we take $R = O_K$ and $k > 1$, the Module LWR is obtained.

2.9 Hardness of LWE

Hardness of LWE**.** For the hardness of LWE problem, we need the following lemma.

Theorem 2.21 ([Reg05, BLP+13])**.** *Let* $\lambda \in \mathbb{N}$ *be a secruity parameter, let* $n, m, q = \mathsf{poly}(\lambda)$ *be lattice parameters. Let* $\chi = D_{\mathbb{Z},\sigma}$ *be a discrete Gaussian distribution with parameter* $\sigma > 2\sqrt{n}$*. There exists an efficient and deterministic reduction from the shortest independent vector problem (*SIVP_γ*) with* $\gamma = \tilde{O}(nq/\sigma)$ *in worst case dimension* n *lattices to the (decision)* $\mathsf{LWE}_{n,m,q,\chi}$ *problem.*

Hardness of RLWE**.** We define the distribution Υ_α over error distributions that was used in the reduction of [PRS17].

Definition 2.22. *For an arbitrary $f(n) = \omega(\sqrt{\log n})$. For $\alpha > 0$, a distribution sampled from Υ_α is an elliptical Gaussian $D_{\boldsymbol{r}}$, where $\boldsymbol{r}$ is sampled as follows: for $i = 1, \cdots, s_1$, sample $x_i \leftarrow D_1$ and set $r_i^2 = \alpha^2(x_i^2 + f^2(n))/2$. for $i = s_1 + 1, \cdots, s_1 + s_2$, sample $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + f^2(n))/2$.*

Then we have the following Theorems:

Theorem 2.23 (Combine [PRS17] and [Pei16b])**.** *Let K be arbitrary number field of degree n, $R = O_K$ and $t \in (R^\vee)^{-1}$ such that $tR^\vee + qR = R$. Let α be the parameter in Definition 2.22, and $\alpha < \omega(\sqrt{\log n/n})$, and let $q \geq 2$ be an integer such that $\alpha q \geq \omega(\sqrt{\log n})$. There exists a polynomial-time quantum reduction from K-SIVP_γ to (average-case,decision) R-$\mathsf{LWE}_{q,t\cdot\Upsilon_\alpha}$ for any*

$$\gamma \leq \max\left\{\omega(\sqrt{n\log n}/\alpha), \sqrt{2}n\right\}.$$

Lemma 2.24 (Combine [PRS17] and [Pei16b])**.** *With the same notations as Theorem 2.23, there is a polynomial-time quantum reduction from K-SIVP_γ to the (average-case, decision) problem of solving R-$\mathsf{LWE}_{q,t\cdot D_\xi}$ using ℓ samples, where*

$$\gamma \leq \left\{\omega(\sqrt{n\log n}/\xi)\cdot(n\ell/\log(n\ell))^{1/4}, \sqrt{2}n\right\}.$$

Hardness of Module-RLWE**.** For the hardness of Module-RLWE, we have the following Lemma.

Lemma 2.25 ([PP19])**.** *Let K be a number field and K'/K be a field extension; R be the ring of integers of K; R' be the ring of integers of K' that is a rank-f free R-module with know basis $\mathbf{B}^*$, ϕ' be a distribution over $K'_{\mathbb{R}}$; and q be a positive integer. Then there exists an efficient, deterministic reduction from (decision) $\mathsf{RLWE}_{\ell,q,\phi'}$ with respect to R' to (decision) module-$\mathsf{RLWE}_{\ell,f,q,\phi}$ with respect R, where $\phi = \mathrm{Tr}_{K'_{\mathbb{R}}/K_{\mathbb{R}}}(\phi')$.*

Hardness of HNFLWE**.** For the hardness of HNFLWE, the following lemma holds.

Lemma 2.26 (Lemma 2 in [ACPS09])**.** *Let $\lambda \in \mathbb{N}$ be a secruity parameter, let $n, q = \mathsf{poly}(\lambda)$ be lattice parameters. Let χ be any error distribution. There exists an efficient and classical reduction from (decision) $\mathsf{LWE}_{n,q,\chi}$ problem to $\mathsf{HNFLWE}_{n,q,\chi}$ problem.*

2.10 Entropic RLWE and Noise Lossiness

In this part, we first recall the definition of entropic RLWE problem in [BD20b], then present the hardness reduction in [BD20b].

Definition 2.27 ((Search) Entropic RLWE [BD20b])**.** *Let R be a ring of integers of a number field K, q be a modulus and n, ℓ be integers. Let χ be an error distribution on $K_{\mathbb{R}}$, $\mathcal{S}$ be a distribution on R_q. The $\mathsf{ent\text{-}sRLWE}_{\ell,q,\chi,\mathcal{S}}$ problem is given ℓ samples $((a_1, b_1), \cdots, (a_\ell, b_\ell))$ from $A_{s,\chi}$, where $s \xleftarrow{\$} \mathcal{S}$, find s.*

We say that the $\mathsf{ent\text{-}sRLWE}_{\ell,q,\chi,\mathcal{S}}$ problem is (standard) hard, if it holds for every PPT adversary $\mathcal{A}$ that

$$\Pr\left[\mathcal{A}\left((a_1, \cdots, a_\ell), \{a_i \cdot s + e_i\}_{i\in\{1,\cdots,\ell\}}\right) = s\right] \leq \mathsf{negl}(\lambda),$$

where $e_i \xleftarrow{\$} \chi, a_i \xleftarrow{\$} R_q$, and $s \xleftarrow{\$} \mathcal{S}$.

For the hardness of entropic RLWE, [BD20b] presented a reduction from DSPR and RLWE to entropic RLWE for power-of-two cyclotomic ring. To this end, let's recall the Decisional Small Polynomial Ratio (DSPR) problem, as defined by Lopez-Alt et al. [LTV12], the lossiness model called *noise lossiness* considered in [BD20b] and some lower bounds of *noise lossiness*.

Definition 2.28 (Decisional Small Polynomial Ratio Problem (DSPR))**.** *Let R be a ring of integers of a number field K and let q be a modulus. Let $\gamma > 0$. Let $g \xleftarrow{\$} D_{R,\gamma}$ and $f \xleftarrow{\$} D_{R,\gamma}$ conditioned on $f \bmod q \in R_q^\times$. Let h be the R_q-inverse of f. The DSPR problem for distribution $D_{R,\gamma}$ asks to distinguish $hg \in R_q$ from a uniformly random $a \xleftarrow{\$} R_q$.*

Definition 2.29 (Noise Lossiness [BD20a])**.** *Let $\mathcal{S} \subseteq \mathbb{Z}_q^n$ be a distribution of secrets, $\mathbf{B} \in \mathbb{R}^{n\times n}$ be a real matrix, and $\sigma > 0$ be a gaussian parameter. The noise-lossiness measure denoted by $v_{\sigma\mathbf{B}}(\mathcal{S})$ is defined by*

$$v_{\sigma\mathbf{B}}(\mathcal{S}) = H_\infty(\boldsymbol{s}|\boldsymbol{s}+\boldsymbol{e}),$$

where $\boldsymbol{s} \xleftarrow{\$} \mathcal{S}$ and $\boldsymbol{e} \xleftarrow{\$} D_{\sigma\mathbf{B}}$.

Lemma 2.30 (General Distributions [BD20a])**.** *Let $\sigma > 0$ be a gaussian parameter, q be a modulo such that $q \geq \frac{\sigma}{\sqrt{\pi/\log(4n)}}$, $\mathcal{S}$ be any distribution on $\mathbb{Z}_q^n$. Then it holds that*

$$v_\sigma(\mathcal{S}) \geq H_\infty(\mathcal{S}) - n\cdot\log(q/\sigma) - 1.$$

Lemma 2.31 (Bounded Distributions [BD20a])**.** *Let $\sigma > 0$ be a gaussian parameter, $\mathcal{S}$ be a r-bounded (ℓ_2 norm) distribution on $\mathbb{Z}_q^n$. Then it holds that*

$$v_\sigma(\mathcal{S}) \geq H_\infty(\mathcal{S}) - \sqrt{2\pi n}\log(e)\cdot\frac{r}{\sigma}.$$

Then, we have the following reduction for the hardness of entropic RLWE [BD20b].

Theorem 2.32. *Assume that* DSPR *with parameter γ and* RLWE *with a B-bounded noise distribution χ holds. Let $\mathcal{S}$ be a distribution such that $v_\sigma(\mathcal{S}) \geq n\log(\gamma\cdot\sqrt{n}\log(n)) + \omega(\log(\lambda))$ for some parameter σ. Then* entSLWE *for power-of-two cyclotomics with $\ell \geq 2n\log q + \omega(\log(\lambda))$ samples, secret distribution $\mathcal{S}$ and error distribution Φ_{bin} is standard hard, where Φ_{bin} is defined as the distribution determined by choosing ℓ elements $e_1, \cdots, e_\ell$ from Gaussian distribution χ with parameter $\sigma_0 \geq O(\sigma n\log(n)\sqrt{\ell}B)$ and $\boldsymbol{x} \xleftarrow{\$} \{0,1\}^\ell$, and outputting $\sum_i x_i$.*

Remark 2.33. *We note that the entropic* RLWE *considered in Corollary 2.32 is with continuous error distribution over $K_\mathbb{R}/qR$. However, we require the error distribution of entropic* RLWE *to be discrete in our later application. Fortunately, there exists a simple reduction from entropic* RLWE *with continuous error distribution to the one with discrete error distribution by making use of the randomized rounding procedure in [Pei10].*

Corollary 2.34. *Assume that* DSPR *with parameter γ and* RLWE *with a B-bounded noise distribution χ holds. Let $\mathcal{S}$ be a distribution such that $v_\sigma(\mathcal{S}) \geq n\log(\gamma\cdot\sqrt{n}\log(n)) + \omega(\log(\lambda))$ for some parameter σ. Then* entSLWE *for power-of-two cyclotomics with $\ell \geq 2n\log q + \omega(\log(\lambda))$ samples, secret distribution $\mathcal{S}$ and error distribution Φ_{bin} defined as Theorem 2.32 above for discrete Gaussian distribution χ with parameter $\sigma_0 \geq O(\sigma n\log^2(n)\sqrt{\ell}B)$ is standard hard.*

2.11 Leftover hash lemma

We will use the following two variants of the leftover hash lemma. Particularly, the first one is with respect to the case of $\mathbb{Z}$, and the second one is related to the case of O_K.

Lemma 2.35 (Particular case of Lemma 2.3 in [MM11])**.** *Let $m, n, q \in \mathbb{N}$ be integers and $\varepsilon \in (0,1)$. Suppose $\boldsymbol{s}$ is chosen from some distribution over $\mathbb{Z}_q^n$ and $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$, $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^m$ are chosen independently of $\boldsymbol{s}$ from uniform distribution. Furthermore let Y be a random-variable (possibly) correlated with $\boldsymbol{s}$.*

- *If q is a prime, and $H_\infty(\boldsymbol{s} \bmod q \mid Y) \geq m\log q + 2\log\left(\frac{1}{\varepsilon}\right)$. Then we have: $\Delta[(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{s}, Y); (\mathbf{A}, \boldsymbol{u}, Y)] \leq \varepsilon$.*
- *If q is a composite number, and $H_\infty(\boldsymbol{s} \bmod p \mid Y) \geq 2m\log q + 2\log\left(\frac{1}{\varepsilon}\right)$ for any factor p of q. Then we have: $\Delta[(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{s}, Y); (\mathbf{A}, \boldsymbol{u}, Y)] \leq \varepsilon$.*

Lemma 2.36 (Generalization of Corollary 5.7 in [LW20])**.** *Let k, e, q be integers, $\varepsilon \in (0,1)$, and $R = O_K$ be the ring of integers of a number field $K = \mathbb{Q}(\alpha)$ with degree n, such that $\gcd(q, [O_K : \mathbb{Z}[\alpha]]) = 1$ and $e \geq 2\log\left(\frac{1}{\varepsilon}\right) + 2n\log q - 2$. Suppose $\boldsymbol{s}$ is chosen from some distribution $\mathcal{X}$ over $(R_q)^k$ and Y be a random-variable (possibly) correlated with $\boldsymbol{s}$, such that $H_\infty(\boldsymbol{s} \bmod \mathfrak{q} \mid Y) \geq e$ for any ideal $\mathfrak{q} | qR$, and $\boldsymbol{a} \xleftarrow{\$} (R_q)^k, u \xleftarrow{\$} R_q$ are uniformly random and independent of $\boldsymbol{s}$. Then we have that $\Delta\big[(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s}\rangle \bmod qR, Y), (\boldsymbol{a}, u, Y)\big] \leq \varepsilon$.*

2.12 Lossy Trapdoor Functions

Definition 2.37 ([PW08, AKPW13])**.** *An lossy trapdoor function (LTF) scheme LTF with preimage distribution $\mathcal{S}$ and image set $\mathcal{Y}$ includes the following algorithms:*

- ***Injective Key Generation.*** $\mathsf{LTF.IGen}(1^\lambda)$ *generates an injective evaluation key* ek *and its corresponding inversion key* ik.
- ***Lossy Key Generation.*** $\mathsf{LTF.LGen}(1^\lambda)$ *generates an lossy evaluation key* ek'.
- ***Evaluation.*** $\mathsf{LTF.Eval}(\mathsf{ek}, \boldsymbol{s})$ *inputs an (injective or lossy) evaluation key and a preimage $\boldsymbol{s} \in \mathcal{S}$, and outputs the image $\boldsymbol{y} = f_{\mathsf{ek}}(\boldsymbol{s})$.*
- ***Inversion.*** $\mathsf{LTF.Invert}(\mathsf{ik}, \boldsymbol{y})$ *inputs an inversion key* ik *and $y \in \mathcal{Y}$, and outputs the unique preimage $\boldsymbol{s} = f_{\mathsf{ik}}^{-1}(\boldsymbol{y})$ such that $\boldsymbol{y} = f_{\mathsf{ek}}(\boldsymbol{s})$.*

We discuss the following properties of LTF*:*

- ***Correctness.*** *For key pair $(\mathsf{ek}, \mathsf{ik}) \leftarrow \mathsf{LTF.IGen}(1^\lambda)$, we require that for all $\boldsymbol{s} \in \mathcal{S}$, with overwhelming probability over $\mathsf{LTF.IGen}(1^\lambda)$ that $x = f_{\mathsf{ik}}^{-1}(f_{\mathsf{ek}}(x))$.*
- ***Expansion.*** *We define the expansion of LTF as $\chi := \log|\mathcal{Y}|/\log|\mathcal{S}|$ and we expect it to be a constant.*
- ***l-Lossiness.*** *We define that a LTF with l-lossiness (abbreviated by l-LTF) satisfies that for mutually correlated random variables $(\boldsymbol{s}, \mathsf{aux})$, $\mathsf{ek}' \leftarrow \mathsf{LTF.LGen}(1^\lambda)$ we have*

$$H_\infty^{\mathsf{smooth}}(\boldsymbol{s} \mid \mathsf{ek}', f_{\mathsf{ek}'}(\boldsymbol{s}), \mathsf{aux}) \geq H_\infty^{\mathsf{smooth}}(\boldsymbol{s} \mid \mathsf{aux}) - l(\lambda)$$

- ***Key Indistinguishability.*** *The distribution of injective evaluation key from* $\mathsf{LTF.IGen}(1^\lambda)$ *is computationally indistinguishable from the distribution of lossy evaluation key from* $\mathsf{LTF.LGen}(1^\lambda)$*, i.e. for any PPT adversary* $\mathcal{A}$

$$\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{LTF},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}(1^\lambda, \mathsf{ek}) = 1\right] - \Pr\left[\mathcal{A}(1^\lambda, \mathsf{ek}') = 1\right]\right|$$

is negligible, with probability under $(\mathsf{ek}, \mathsf{ik}) \leftarrow \mathsf{LTF.IGen}(1^\lambda)$ *and* $\mathsf{ek}' \leftarrow \mathsf{LTF.LGen}(1^\lambda)$.

3 Entropic Learning with Rounding

In this section, we present a new definition capturing the LWR problem with entropic secret.

Definition 3.1 (Entropic GLWR)**.** *Let* R *be a sub-ring of a number field* K*,* $q = q(\lambda) \geq p = p(\lambda) \geq 2$*,* $k = k(\lambda) \geq 1$ *and* $m = m(\lambda) > 1$ *be positive integers, and* $\mathbf{B}$ *be a basis of* R*. Let* $\mathcal{S}$ *be a distribution on* $(R_q)^k$*. We say that the search problem* $\mathsf{ent\text{-}sGLWR}(q, p, \mathbf{B}, k, m, \mathcal{S})$ *is hard, if it holds for every* PPT *adversary* $\mathcal{A}$ *we have that*

$$\mathsf{Adv}^{k,m,q,p,\mathbf{B},\mathcal{S}}_{\mathsf{ent\text{-}sGLWR},\mathcal{D}}(\lambda) := \mathsf{Pr}[\mathcal{A}(1^\lambda, \mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}) = \boldsymbol{s}] \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \xleftarrow{\$} (R_q)^{m\times k}, \boldsymbol{s} \xleftarrow{\$} \mathcal{S}$*. Similarly, the decisional problem* $\mathsf{ent\text{-}dGLWR}(q, p, \mathbf{B}, k, m, \mathcal{S})$ *is hard, if it holds for every* PPT *distinguisher* $\mathcal{D}$ *we have that*

$$\mathsf{Adv}^{k,m,q,p,\mathbf{B},\mathcal{S}}_{\mathsf{ent\text{-}dGLWR},\mathcal{D}}(\lambda) := \left|\mathsf{Pr}[\mathcal{D}(1^\lambda, \mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}) = 1] - \mathsf{Pr}[\mathcal{D}(1^\lambda, \mathbf{A}, \boldsymbol{u}) = 1]\right| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \xleftarrow{\$} (R_q)^{m\times k}, \boldsymbol{s} \xleftarrow{\$} \mathcal{S}$ *and* $\boldsymbol{u} \xleftarrow{\$} (R_p)^m$.

3.1 Rounding Lossiness

In order to analyse the hardness of Entropic LWR, we introduce a new measure called *rounding lossiness*, that describes the remaining entropy of the distribution conditioned on the deterministic rounding of this distribution. We also provide some useful lower bounds of these measures in various cases.

Definition 3.2 (Rounding Lossiness over $\mathbb{Z}_q^k$)**.** *Let* $q \geq p^* \geq 2$ *be integers and let* $\mathcal{S} \subseteq \mathbb{Z}_q^k$ *be a distribution of secrets. We define the rounding-lossiness* $\mathcal{R}_{q,p^*}(\mathcal{S})$ *by*

$$\mathcal{R}_{q,p^*}(\mathcal{S}) = H_\infty\left(\boldsymbol{s} \mid \lfloor \boldsymbol{s} \rceil_{q,p^*}\right), \text{ where } \boldsymbol{s} \xleftarrow{\$} \mathcal{S}$$

Similarly, for any integer $p' < q$*,* $\mathcal{R}_{q,p^*}(\mathcal{S} \bmod p')$ *is defined by*

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod p') = H_\infty\left(\boldsymbol{s} \bmod p' \mid \lfloor \boldsymbol{s} \rceil_{q,p^*}\right), \text{ where } \boldsymbol{s} \xleftarrow{\$} \mathcal{S}.$$

In the case of the ring, we similarly define the rounding lossiness with respect to specific basis.

Definition 3.3 (Rounding Lossiness over $(O_K)_q^k$)**.** *Let* $R = O_K$ *be the ring of integers of a number field* K*,* $\mathbf{B}$ *be a basis of* R*,* $q \geq p^* \geq 2$ *and* $k \geq 1$ *be integers. Let* $\mathcal{S} \subseteq (R_q)^k$ *be a distribution of secrets. We define the rounding-lossiness* $\mathcal{R}_{\mathbf{B},q,p^*}(\mathcal{S})$ *by*

$$\mathcal{R}_{\mathbf{B},q,p^*}(\mathcal{S}) = H_\infty\left(\boldsymbol{s} \mid \lfloor \boldsymbol{s} \rceil_{\mathbf{B},q,p^*}\right), \text{ where } \boldsymbol{s} \xleftarrow{\$} \mathcal{S}$$

Similarly, for any prime ideal factor $\mathfrak{q}$ *of* qR*,* $\mathcal{R}_{q,p^*}(\mathcal{S} \bmod \mathfrak{q})$ *is defined by*

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod \mathfrak{q}) = H_\infty\left(\boldsymbol{s} \bmod \mathfrak{q} \mid \lfloor \boldsymbol{s} \rceil_{\mathbf{B},q,p^*}\right), \text{ where } \boldsymbol{s} \xleftarrow{\$} \mathcal{S}.$$

It can easily obtain the following useful lemmas lower bound the rounding lossiness in various cases. To start, we consider the case of $\mathbb{Z}_q^n$ for arbitrary entropic distribution.

Lemma 3.4 (Rounding-Lossiness for General Entropic Distributions)**.** *Let $q \geq p^* \geq 2$ be integers, and let $\mathcal{S}$ be any distribution on $\mathbb{Z}_q^k$. Then we have*

$$\mathcal{R}_{q,p^*}(\mathcal{S}) \geq H_\infty(\mathcal{S}) - k \log p^*.$$

Similarly, for any integer $p' < q$, it holds that

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod p') \geq H_\infty(\mathcal{S} \bmod p') - k \log p^*.$$

For the case of $(O_K)_q^k$, we have the following analogous lemma.

Lemma 3.5. *Let $R = O_K$ be the ring of integers of a number field K with degree n, $\mathbf{B}$ be a basis of R, $q \geq p^* \geq 2$ and $k \geq 1$ be integers. Let $\mathcal{S}$ be any distribution on $(R_q)^k$. Then it holds that*

$$\mathcal{R}_{q,p^*}(\mathcal{S}) \geq H_\infty(\mathcal{S}) - nk \log p^*.$$

Similarly, for any prime ideal factor $\mathfrak{q}$ of qR, it holds that

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod \mathfrak{q}) \geq H_\infty(\mathcal{S} \bmod \mathfrak{q}) - nk \log p^*.$$

When considering the bounded entropic distribution, we have the following lemma for the case of $\mathbb{Z}_q^n$.

Lemma 3.6 (Rounding-Lossiness for Bounded Distributions)**.** *Let $q \geq p^* \geq 2$ be integers, and let $\mathcal{S}$ be a γ-bounded distribution on $\mathbb{Z}_q^k$. Then it holds that*

$$\mathcal{R}_{q,p^*}(\mathcal{S}) \geq H_\infty(\mathcal{S}) - k \log \left(2 \left\lfloor \frac{\gamma p^*}{q} \right\rfloor + 1\right).$$

Similarly, for any integer $p' < q$, it holds that

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod p') \geq H_\infty(\mathcal{S} \bmod p') - k \log \left(2 \left\lfloor \frac{\gamma p^*}{q} \right\rfloor + 1\right).$$

Similarly, we can also obtain the lower bound of rounding lossiness for bounded entropic distribution over ring. Before stating the lemma, we should define the bounded distribution over the rings.

Definition 3.7 (Bounded Distributions over $(O_K)_q^k$ Relative to Basis)**.** *Let $R = O_K$ be the ring of integers of a number field K with degree n, $\mathbf{B}$ be a basis of R, $k \geq 1$ be a integer. We call a distribution $\mathcal{S} \subseteq (R_q)^k$ γ-bounded relative to basis $\mathbf{B}$, if for any $\mathbf{s} = (s_1, \cdots, s_k) \leftarrow \mathcal{S}$, each coefficient $s_i[j]$ of each s_i relative to $\mathbf{B}$ has range in $[-\gamma, \gamma]$ for $i \in [k], j \in [n]$.*

Then the following lemma can be similarly obtained by dropping the information bits of leakage.

Lemma 3.8. *Let $R = O_K$ be the ring of integers of a number field K with degree n, $\mathbf{B}$ be a basis of $\mathcal{L}^\vee$, $q \geq p^* \geq 2$ be integers. Let $\mathcal{S}$ be a γ-bounded distribution over $(R_q)^k$ relative to basis $\mathbf{B}$. Then it holds that*

$$\mathcal{R}_{q,p^*}(\mathcal{S}) \geq H_\infty(\mathcal{S}) - nk \log \left(2 \left\lfloor \frac{\gamma p^*}{q} \right\rfloor + 1\right).$$

Similarly, for any prime ideal factor $\mathfrak{q}$ of qR, it holds that

$$\mathcal{R}_{q,p^*}(\mathcal{S} \bmod \mathfrak{q}) \geq H_\infty(\mathcal{S} \bmod \mathfrak{q}) - nk \log \left(2 \left\lfloor \frac{\gamma p^*}{q} \right\rfloor + 1\right).$$

4 New Hardness Results of Entropic LWR

In this section, we present our new hardness results of Entropic LWR. First we show a core lemma that relates the hardness of Entroic LWR to the the rounding lossiness proposed in Section 3. Then we establish the hardness of Entropic LWR from LWE by assuming the rounding lossiness is sufficient. Finally, we provide a comparison between our rounding lossiness approach and the noise lossiness approach in [BD20a]. Our reduction can also be generalized to the Entropic MLWR case, and we put this part to Appendix C. Before presenting the core lemma, we first recall a useful tool in our analysis and provide the security of it.

Definition 4.1 (Lossy Sampler, Definition 3.1 in [AKPW13])**.** *Let λ be the security parameter, n, m, ℓ, q be integers (functions of λ), and $\chi = \chi(\lambda)$ be a distribution over $\mathbb{Z}_q$. We define the lossy sampler $\tilde{\mathbf{A}} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$ as:*

$\mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$: *Sample* $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m\times\ell}$, $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{\ell\times n}$, $\mathbf{F} \leftarrow \chi^{m\times n}$ *and output* $\tilde{\mathbf{A}} = \mathbf{B}\cdot\mathbf{C} + \mathbf{F}$.

Lemma 4.2. *Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$, and let $\tilde{\mathbf{A}} \xleftarrow{\$} \mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$. Then, under the $\mathsf{LWE}_{\ell,m,q,\chi}$ assumption, we have: $\mathbf{A} \overset{c}{\approx} \tilde{\mathbf{A}}$.*

Lemma 4.3. *Let $n, m, \ell, p, p^*, q, \beta$ be positive integers such that $q > p^* \geq nmp\beta$, and χ be a β-bounded distribution over $\mathbb{Z}_q$. Let $(\boldsymbol{s}, \mathsf{aux})$ be a pair of correlated random variables with $\boldsymbol{s}$ distributed according to some distribution $\mathcal{S} \subseteq \mathbb{Z}_q^n$ and $\Pr_{\boldsymbol{s}}\left[\boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*\right] < \delta$, and let $\tilde{\mathbf{A}}$ be a matrix independently output by the algorithm $\mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$. Then for $\varepsilon = 2^{-\lambda} + \delta + 2^{-\ell+1}$, any $\varepsilon' > 0$ and any every function f taken input over $\mathcal{S}$, we have:*

$$H_\infty^{\varepsilon'+\varepsilon}(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p, \mathsf{aux}) \geq H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \lfloor \boldsymbol{s}\rceil_{q,p^*}, \mathsf{aux}) - (\ell+\lambda)\log q.$$

Proof. According to Definition 4.1, $\tilde{\mathbf{A}}$ can be written as $\tilde{\mathbf{A}} = \mathbf{B}\cdot\mathbf{C} + \mathbf{F}$, then $\lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p = \lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \mathbf{F}\cdot\boldsymbol{s}\rceil_p$. Furthermore, $\lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \mathbf{F}\cdot\boldsymbol{s}\rceil_p$ can be written as

$$\lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \mathbf{F}\cdot\boldsymbol{s}\rceil_p = \left\lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \frac{q}{p^*}\mathbf{F}\cdot\lfloor\boldsymbol{s}\rceil_{p^*} + \frac{q}{p^*}\mathbf{F}\left(\frac{p^*}{q}\boldsymbol{s} - \lfloor\boldsymbol{s}\rceil_{p^*}\right)\right\rfloor_p.$$

We define the set $I \overset{\text{def}}{=} \left\{i \in [m] : \left\lfloor \left(\mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \frac{q}{p^*}\mathbf{F}\cdot\lfloor\boldsymbol{s}\rceil_{p^*}\right)_i\right\rceil_p \neq \left\lfloor \left(\tilde{\mathbf{A}}\cdot\boldsymbol{s}\right)_i\right\rceil_p\right\}$, where $(\boldsymbol{x})_i$ denotes i-th coordinate of $\boldsymbol{x}$. Let $Z = \left\{\left(i, \left\lfloor \left(\tilde{\mathbf{A}}\cdot\boldsymbol{s}\right)_i\right\rceil_p\right) : i \in I\right\}$, and it is not hard to see that $(\tilde{\mathbf{A}}, \lfloor\tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p)$ can be reconstructed completely given $\mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*}\lfloor\boldsymbol{s}\rceil_{p^*}, Z$. Therefore:

$$H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \lfloor\tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p, \mathsf{aux}\right) \geq H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*}\lfloor\boldsymbol{s}\rceil_{p^*}, Z, \mathsf{aux}\right).$$

Next we show a lower bound for the right hand side by bounding the min-entropy loss given Z. To do this, we first bound the probability that the size of I is large:

Claim 4.4. $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda] < \delta + 2^{-\ell+1} + 2^{-\lambda}$.

Proof. We can divide the event $|I| > \lambda$ into two conditions: $\boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*$ and $\boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*$ and obtain:

$$\begin{aligned}\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda\right] &= \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*\right] \cdot \Pr_{\boldsymbol{s}}\left[\boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*\right] \\ &+ \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \cdot \Pr_{\boldsymbol{s}}\left[\boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \\ &\leq \Pr_{\boldsymbol{s}}\left[\boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*\right] + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right].\end{aligned} \tag{1}$$

Then, we have

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda\right] < \delta + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right].$$

So our next step is to bound $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right]$.

For any $\boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*$ and independently chosen matrix $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{\ell \times n}$, $\mathbf{C} \cdot \boldsymbol{s}$ is uniformly distributed over $\mathbb{Z}_q^\ell$. Thus by the lower bound of $\left|(\mathbb{Z}_q^\ell)^*\right|$,

$$\Pr_{\mathbf{C},\boldsymbol{s}}\left[\mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \geq 1 - 2^{-\ell+1}.$$

Now we further divide $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right]$ into two cases as follows:

$$\begin{aligned}&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \\ &= \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C} \cdot \boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^*\right] \cdot \Pr_{\mathbf{C},\boldsymbol{s}}\left[\mathbf{C} \cdot \boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \\ &+ \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] \cdot \Pr_{\mathbf{C},\boldsymbol{s}}\left[\mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right].\end{aligned}$$

Combining the above equation with (1), we have

$$\begin{aligned}&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda\right] \\ &< \delta + \Pr_{\mathbf{C},\boldsymbol{s}}\left[\mathbf{C} \cdot \boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] \\ &< \delta + 2^{-\ell+1} + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right].\end{aligned} \tag{2}$$

It's easy to see

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] = \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right]$$

as $\mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*$ implies $\boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*$, so it's remain to bound $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[|I| > \lambda \mid \mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right]$.

To do this, we denote the i-th column of the matrices $\mathbf{B}$ and $\mathbf{F}$ as as $\boldsymbol{b}_i$ and $\boldsymbol{f}_i$, respectively. We fix $\boldsymbol{s}$ and $\mathbf{C}$ such that $\mathbf{C} \cdot \boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*$, and compute $\Pr[|I| > \lambda \mid \mathbf{C}, \boldsymbol{s}]$. For simplicity, we omit the condition $\mathbf{C}$ and $\boldsymbol{s}$

below as they are fixed now. Then, according to our definition of I, we have for every $i \in [m]$:

$$\begin{aligned}
&\Pr_{\mathbf{B},\mathbf{F}}[i \in I] = \Pr_{\mathbf{B},\mathbf{F}}\left[\lfloor(\tilde{\mathbf{A}}\cdot \boldsymbol{s})_i\rceil_p \neq \left\lfloor \left(\mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \frac{q}{p^*}\mathbf{F}\cdot\lfloor \boldsymbol{s}\rceil_{p^*}\right)_i \right\rceil_p \right] \\
&= \Pr_{\boldsymbol{b}_i \boldsymbol{f}_i}\left[\left\lfloor \langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{b}_i\rangle + \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle + \frac{q}{p^*}\left\langle \boldsymbol{f}_i, \frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s}\rceil_{p^*}\right\rangle \right\rceil_p \neq \left\lfloor \langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{b}_i\rangle + \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle \right\rceil_p \right] \\
&\leq \Pr_{\boldsymbol{b}_i \boldsymbol{f}_i}\left[\langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{b}_i\rangle + \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle \in \mathsf{border}_{p,q,\nu}\left(\left|\frac{q}{p^*}\left\langle \boldsymbol{f}_i, \frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s}\rceil_{p^*}\right\rangle\right|\right)\right] \qquad (3) \\
&= \sum_{\tau}\Pr_{\boldsymbol{f}_i}\left[\left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle\right| = \tau \right] \Pr_{\boldsymbol{b}_i \boldsymbol{f}_i}\left[\langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{b}_i\rangle + \frac{q}{p^*}\left\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle \in \mathsf{border}_{p,q,\nu}(\tau)\right] \\
&\leq \sum_{\tau}\Pr_{\boldsymbol{f}_i}\left[\left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle\right| = \tau \right] \cdot \frac{2\tau p}{q} \qquad (4) \\
&= \mathbf{E}_{\boldsymbol{f}_i}\left[\left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle\right| \right] \cdot \frac{2p}{q} \\
&\leq \frac{np\beta}{p^*} \leq \frac{1}{m}. \qquad (5)
\end{aligned}$$

where $\nu = \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle - \lfloor \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle \rfloor$ and (3) follows from the definition of a "border", (4) follows by Lemma 2.3 and the uniformity of $\langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{b}_i\rangle$ over $\mathbb{Z}_q$, and (5) follows since each entry of $\boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}$ is bounded by $\frac{q}{2p^*}$ in absolute value, and each entry of $\boldsymbol{f}_i$ is bounded by β in absolute value.

From the above, we have that

$$\mathbf{E}[|I|] = \sum_{i\in[m]}\mathbf{E}[i \in I] = \sum_{i\in[m]}\Pr[i \in I] \leq 1.$$

Furthermore for $i \in [m]$, the events $i \in I$ are mutually independent, as their probabilities are based on independently chosen $\boldsymbol{b}_i$'s and $\boldsymbol{f}_i$'s. Therefore, by the Chernoff bound, we have

$$\Pr_{\mathbf{B},\mathbf{F}}\left[|I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] < 2^{-\lambda},$$

for any fixed $\boldsymbol{s}, \mathbf{C}$ satisfying the condition. Using Equation (2) and the above calculation, we have

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda] < \delta + 2^{-\ell+1} + 2^{-\lambda}.$$

This completes the proof. □

The bit-length of Z is $|I|(\log m + \log p)$, which is upper-bounded by $\lambda(\log m + \log p)$ with overwhelming probability, i.e., $1 - \varepsilon = 1 - (\delta + 2^{-\ell+1} + 2^{-\lambda})$. Therefore, we have

$$\begin{aligned}
H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \lfloor\tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p, \mathsf{aux}\right) &\geq H_\infty^{\varepsilon'+\varepsilon}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\cdot\boldsymbol{s}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, Z, \mathsf{aux}) \\
&\geq H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\cdot\boldsymbol{s}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \mathsf{aux}) - \lambda(\log m + \log p) \\
&\geq H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \mathsf{aux}) - \ell\log q - \lambda(\log m + \log p) \\
&\geq H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \mathsf{aux}) - (\ell+\lambda)\log q \\
&= H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \lfloor \boldsymbol{s}\rceil_{p^*}, \mathsf{aux}) - (\ell+\lambda)\log q.
\end{aligned}$$

where the second and the third lines follow by Lemma 2.8 and Claim 4.4, and the last line follows by $q \geq p^* \geq mp$. This completes the proof of Lemma 4.3. □

Now we can formally present the hardness results of entropic LWR according to the following theorem.

Theorem 4.5. *Let $n, m, \ell, p, p^*, q, \beta$ be positive integers such that $q > p^* \geq \beta nmp$, χ be a β-bounded distribution over $\mathbb{Z}_q$ and $\mathcal{S}$ be a distribution on $\mathbb{Z}_q^n$. Then we have the following:*

- *There exists a poly-time reductions from $\mathsf{LWE}_{\ell,m,q,\chi}$ to $\mathsf{ent\text{-}dLWR}(q,p,k,m,\mathcal{S})$, for which q is a prime and $\mathcal{R}_{q,p^*}(\mathcal{S}) \geq (\ell+\lambda+1)\cdot\log(q)+\omega(\log(\lambda))$.*
- *There exists a poly-time reductions from $\mathsf{LWE}_{\ell,m,q,\chi}$ to $\mathsf{ent\text{-}dLWR}(q,p,k,m,\mathcal{S})$, for which q is a composite number and $\mathcal{R}_{q,p^*}(\mathcal{S} \bmod p_i) \geq (\ell+\lambda+2)\cdot\log(q)+\omega(\log(\lambda))$ for any factor p_i of q.*

Proof. The proof of this Theorem follows roughly the same idea of the work [AKPW13]. We only prove the first result of the theorem. The proof of the second result works in complete analogy.

Our target is to prove the following: under $\mathsf{LWE}_{\ell,m,q,\chi}$ assumption with parameters in the theorem, we have

$$\left(\begin{bmatrix} \mathbf{A} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \mathbf{A}\boldsymbol{s} \rceil_p \\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_p \end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix} \mathbf{A} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \mathbf{A}\boldsymbol{s} \rceil_p \\ \lfloor u \rceil_p \end{bmatrix} \right) \tag{6}$$

where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n, \boldsymbol{s} \xleftarrow{\$} \mathcal{S}, u \xleftarrow{\$} \mathbb{Z}_p$.

By Lemma 4.2, we can replace the uniformly random $\mathbf{A}$ with lossy $\tilde{\mathbf{A}}$ to obtain

$$\left(\begin{bmatrix} \mathbf{A} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \mathbf{A}\boldsymbol{s} \rceil_p \\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_p \end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix} \tilde{\mathbf{A}} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \tilde{\mathbf{A}}\boldsymbol{s} \rceil_p \\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_p \end{bmatrix} \right)$$

By Lemma 4.3, for $\varepsilon = 2^{-\lambda} + \delta + 2^{-\ell+1}$ and any $\varepsilon' > 0$, we have:

$$\begin{aligned} H_\infty^{\varepsilon'+\varepsilon}(\boldsymbol{s} \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s} \rceil_p) &\geq H_\infty^{\varepsilon'}(\boldsymbol{s} \mid \lfloor \boldsymbol{s} \rceil_{q,p^*}) - (\ell+\lambda)\log(q) \\ &\geq (\ell+\lambda+1)\cdot\log(q) + \omega(\log(\lambda)) - (\ell+\lambda)\log(q) \\ &\geq \log(q) + \omega(\log(\lambda)). \end{aligned}$$

On the other hand, it's clear that $H_\infty(\boldsymbol{s}) \geq H_\infty(\boldsymbol{s} \mid \lfloor \boldsymbol{s} \rceil_{q,p^*}) \geq (\ell+\lambda+1)\cdot\log(q) + \omega(\log(\lambda))$. Then $\Pr\left[\, \boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^* \,\right] = \Pr[\, \boldsymbol{s} = \mathbf{0} \,] \leq q^{-(\ell+\lambda+1)} \cdot 2^{-\omega(\log\lambda)} < q^{-\lambda}$, which means that δ can be set as $q^{-\lambda}$, and thus $\varepsilon = 2^{-\lambda} + q^{-\lambda} + 2^{-\ell+1}$.

Combining above with leftover hash lemma as Lemma 2.35, we have

$$\left(\begin{bmatrix} \tilde{\mathbf{A}} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \tilde{\mathbf{A}}\boldsymbol{s} \rceil_p \\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_p \end{bmatrix} \right) \overset{s}{\approx} \left(\begin{bmatrix} \tilde{\mathbf{A}} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \tilde{\mathbf{A}}\boldsymbol{s} \rceil_p \\ \lfloor u \rceil_p \end{bmatrix} \right).$$

The exact statistical distance is bounded by $2^{-\omega(\log\lambda)}$. Finally, we replace the lossy $\tilde{\mathbf{A}}$ with uniformly random $\mathbf{A}$ to get:

$$\left(\begin{bmatrix} \tilde{\mathbf{A}} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \tilde{\mathbf{A}}\boldsymbol{s} \rceil_p \\ \lfloor u \rceil_p \end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix} \mathbf{A} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \mathbf{A}\boldsymbol{s} \rceil_p \\ \lfloor u \rceil_p \end{bmatrix} \right).$$

Combining the above three hybrids proves (6).

By a simple hybrid argument as [AKPW13], we can further prove the desired statement

$$(\mathbf{A}, \lfloor \mathbf{A}\boldsymbol{s} \rceil_p) \overset{c}{\approx} (\mathbf{A}, \lfloor \boldsymbol{u} \rceil_p).$$

□

Remark on Parameters. Note that the parameter p^* in Theorem 4.5 provides a lower bound of the modulus q, and at the same time, p^* also determines the lower bound of the secret's rounding losssiness by Lemma 3.4 and Lemma 3.6. Therefore, for a bigger p^* we need a bigger modulus q to satisfy the constraint in Theorem 4.5, and need more entropy of the secret to meet the requirement of randomness extraction (Lemma 2.35). On the other hand, for a fixed p^*, the entropy requirement of the secret offers a tradeoff between the size of modulus q and the vector length n. When considering the case that $\mathcal{S}$ is the uniformly random distribution, the following corollary presents two extreme cases of small modulus q and small n, which is consistent with the results showed in [AKPW13].

Corollary 4.6. *Let n, m, ℓ, p, q, β be positive integers, χ be a β-bounded distribution over $\mathbb{Z}_q$. Then we have the following:*

- *There exists a poly-time reductions from $\mathsf{LWE}_{\ell,m,q,\chi}$ to $\mathsf{dLWR}(q,p,k,m)$, for which $q \geq 2\beta nmp$ is a prime (or q is a composite), and $n \geq (\ell+\lambda+1)\cdot\log(q) + \omega(\log(\lambda))$ (or $n \geq (\ell+\lambda+2)\cdot\log(q) + \omega(\log(\lambda))$. We can obtain a modulus-to-error ratio as small as $q/\beta = O(m\cdot n)$ if further set $p = O(1)$.*
- *There exists a poly-time reductions from $\mathsf{LWE}_{\ell,m,q,\chi}$ to $\mathsf{dLWR}(q,p,k,m)$, for which $q \geq (\beta nmp)^2$ is a prime (or q is a composite), and $n \geq 2\ell + 4\lambda + 2$ (or $n \geq 2\ell + 4\lambda + 4$). The LWR assumption can achieve similar efficiency as LWE (i.e., $n = O(\ell)$ and $\log(p) = O(\log q)$) if we further set $p = \beta nm$.*

Proof. It follows directly from Theorem 4.5. For case (1), we set $p^* = \beta nmp$, then $q \geq 2p^*$, and thus $\mathcal{R}_{q,p^*}(\mathcal{S}) \geq n$. For case (2), we set $p^* = \sqrt{q} = p^2$, then $\mathcal{R}_{q,p^*}(\mathcal{S}) \geq \frac{n}{2}\cdot\log q$. □

5 Compact Lattice Trapdoor and its Applications to Lossy Trapdoor Functions

In this section, we propose our construction of compact lattice trapdoor, and further present compact lossy trapdoor functions by combining the trapdoor construction and our previous entropic LWR reduction. As a crux analysis in our compact trapdoor design, we first show a theorem about the requirements of a random matrix having an invertible sub-matrix.

5.1 Probability of Matrix with Generalized Invertibility

First of all, we define what it means for a matrix from $\mathbb{Z}_q^{n\times m}$ ($m \geq n$) to be *invertible* for any modulus q. This notion is a generalization of the square matrix's invertibility to a more general case of matrix from $\mathbb{Z}_q^{n\times m}$ ($m \geq n$), and also appeared in several previous works [ACPS09, BD20a].

Definition 5.1. *Let $m' \geq n \geq 1$ be dimension parameters and $q \geq 2$ be any modulus. For a matrix $\mathbf{A} = (\mathbf{a}_i)_{i\in[m']} \in \mathbb{Z}_q^{n\times m'}$, we define that a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m'}$ is invertible if there exists n positive indexes $i_1 < i_2 < \cdots < i_n \leq m'$ such that $\mathbf{H} = (\mathbf{a}_{i_1}|\mathbf{a}_{i_2}|\cdots|\mathbf{a}_{i_n}) \in \mathbb{Z}_q^{n\times n}$ is invertible. We define $\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q}$ to be the probability of a uniformly random matrix in $\mathbb{Z}_q^{n\times m'}$ to be not invertible, i.e., $\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q} = \Pr_{\mathbf{A}\xleftarrow{\$}\mathbb{Z}_q^{n\times m'}}[\mathbf{A} \text{ is not invertible}]$.*

Afterwards, we prove that if m' is slightly larger than n, then the probability $\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q}$ is negligible for arbitrary polynomial-size modulus q.

Theorem 5.2. *For any modulus $q \geq 25$, $n \geq 1$ and $t_1, t_2 \geq 1$, for $m' = n + t_1 + t_2\ln\ln q$, we have $\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q} \leq 2^{-(t_1+1)} + e^{-t_2/4}$.*

Proof. The general idea of this proof is to separate m' uniform and independent vectors from $\mathbb{Z}_q^n$ into former $(n+t_1)$ vectors and latter $t_2 \ln\ln q$ vectors. We then illustrate that 1. there exists $n-1$ linearly independent vectors $\{\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}\}$ in the first $n+t_1$ vectors except with probability 2^{-t_1}; 2. given $n-1$ existing linearly independent vectors, there exists a vector $\mathbf{u}_n$ in the last $t_2 \ln\ln q$ vectors such that $\mathbf{u}_n$ is linearly independent from $\{\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}\}$ except with probability $e^{-t_2/4}$.

Let $q = q_1 q_2 \cdots q_k$ represents the prime factorization of the modulus q where each $q_j = p_j^{d_j}$ is a power of prime. Let $\{\mathbf{u}_i\}_{1 \le i \le n}$ be vectors from $\mathbb{Z}_q^n$. For $1 \le i \le n$, denote E_i as the event that $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i \in (\mathbb{Z}_q^n)^*$ and $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i$ are linearly independent in $\mathbb{Z}_q^n$. We define E_i^j (respectively D_i^j) as the event that $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i \in (\mathbb{Z}_{q_j}^n)^*$ (respectively $(\mathbb{Z}_{p_j}^n)^*$) and these vectors are linearly independent in $\mathbb{Z}_{q_j}^n$ (respectively $\mathbb{Z}_{p_j}^n$) for $1 \le i \le n$ and $1 \le j \le k$. Our next goal is to compute $\Pr_{\mathbf{u}_i}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ for all i where the probability is taken from $\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n$.

Claim 5.3. *We have*

- *If* $1 \le i \le n-1$, $\Pr_{\mathbf{u}_i}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] \ge 1 - 2^{-n+i}$.
- $\Pr_{\mathbf{u}_n}[\mathsf{E}_n \mid \mathsf{E}_{n-1}] = \varphi(q)/q$, *where* φ *is the Euler totient function.*

Proof. First, we can get a lower bound for each $\Pr_{\mathbf{u}_i}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j]$ where the probability is taken from $\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{q_j}^n$. For all $1 \le j \le k$,

$$\begin{aligned}
\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{q_j}^n}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j] &= \Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{p_j}^n}[\mathsf{D}_i^j \mid \mathsf{D}_{i-1}^j] \\
&= \Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{p_j}^n}[\mathbf{u}_i \notin \mathsf{span}\{\mathbf{u}_1, \cdots, \mathbf{u}_{i-1}\} \mid \mathsf{D}_{i-1}^j] \\
&= 1 - \Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{p_j}^n}[\mathbf{u}_i \in \mathsf{span}\{\mathbf{u}_1, \cdots, \mathbf{u}_{i-1}\} \mid \mathsf{D}_{i-1}^j] \\
&= 1 - p_j^{-(n-i+1)}.
\end{aligned}$$

Since the k random variables $(\mathbf{u}_i \bmod q_j)$ for $j \in [k]$ is mutually independent when $\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n$, we observe that for all $1 \le i \le n$,

$$\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] = \prod_{j=1}^{k} \Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_{q_j}^n}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j] = \prod_{j=1}^{k} \left(1 - p_j^{-(n-i+1)}\right).$$

If $1 \le i \le n-1$, by Lemma 2.1 and union bound,

$$\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] \ge 1 - \sum_{j=1}^{k} p_j^{-(n-i+1)} > 1 - 2^{-(n-i)}.$$

For the case $i = n$,

$$\Pr_{\mathbf{u}_n \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_n \mid \mathsf{E}_{n-1}] = \prod_{j=1}^{k} \left(1 - p_j^{-1}\right) = \frac{\varphi(q)}{q}.$$

□

We define the following probabilities

$$P_1 = \Pr_{\mathbf{A}_1 \xleftarrow{\$} \mathbb{Z}_q^{n\times(n+t_1)}} [\exists\ n-1 \text{ linearly independent column vectors in } \mathbf{A}_1],$$

$$P_2 = \Pr_{\mathbf{u}_i' \xleftarrow{\$} \mathbb{Z}_q^n, i\in[t_2 \ln\ln q]} [\exists\ \mathbf{u}_i'\ s.t.\ \mathbf{u}_i' \cup \{\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}\} \text{ is linearly independent} \mid \mathsf{E}_{n-1}]$$

We see that the probability of an matrix from $U(\mathbb{Z}_q^{n\times m})$ to be invertible has a lower bound $1-\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q}(\lambda) \geq P_1P_2$.

Our next target is to prove that P_1 and P_2 are both $1-\mathsf{negl}(\lambda)$. In claim 5.3, we already present a lower bound of probability for each event E_i conditioned on E_{i-1} under the choice $\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n$. In order to utilize these lower bounds to compute P_1, we construct an event with same combinatorial meaning.

Let $\{\mathbf{v}_i\}_{i\in[n-1]}$ be vectors from $\mathbb{Z}_2^{n-1}$. For $1 \leq i \leq n-1$, we denote F_i as the event that $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_i$ are linearly independent in $\mathbb{Z}_2^{n-1}$, and we find that $\Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^{n-1}}[\mathsf{F}_i \mid \mathsf{F}_{i-1}]$ exactly matches the lower bound of $\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ in claim 5.3:

$$\Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^{n-1}}[\mathsf{F}_i \mid \mathsf{F}_{i-1}] = 1 - \frac{2^{i-1}}{2^{n-1}} = 1 - 2^{-(n-i)} \leq \Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]. \tag{7}$$

Let $\mathbf{A}_1 \xleftarrow{\$} \mathbb{Z}_q^{n\times m_1'}$ (respectively $\mathbf{F}_1 \xleftarrow{\$} \mathbb{Z}_2^{(n-1)\times m_1'}$), which contains m_1' independent samples. We can view the process of picking $n-1$ linearly independent column vectors of $\mathbf{A}_1$ (respectively $\mathbf{F}_1$) as tossing irregular coins, where each sample (column vector) represents a toss round and head denotes that a sample vector meets the criteria based on chosen samples. To be detailed, during the process of picking linearly independent vectors from $\mathbf{A}_1$ (respectively $\mathbf{F}_1$), the probability of flipping a coin with a head outcome based on $i-1$ heads is $\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ (respectively $\Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^{n-1}}[\mathsf{F}_i \mid \mathsf{F}_{i-1}]$). It should be noted that, these two scenes have the same number of samples (both m_1), same target number (both $n-1$), and same tossing coins settings (probability of a head is based on the number of existing heads). From the inequality (7), the probability of tossing a coin with a head outcome conditioned on $(i-1)$ existing heads in case of $\mathbf{A}_1$ is greater than or equal to probability in case $\mathbf{F}_1$ for all $i \leq n-1$. Therefore, we can obtain that the probability of $n-1$ heads in $\mathbf{A}_1$ is greater than or equal to the probability in $\mathbf{F}_1$, i.e. P_1 can be lower bounded by the probability of $U(\mathbb{Z}_2^{(n-1)\times(n+t_1)})$ to be invertible:

$$P_1 \geq \Pr_{\mathbf{F}_1 \xleftarrow{\$} \mathbb{Z}_2^{(n-1)\times(n+t_1)}} [\mathbf{F}_1 \text{ is invertible}].$$

Since $\mathbb{Z}_2$ is a field, $\mathbf{F}_1$ is invertible iff $\mathbf{F}_1$ has column rank $n-1$ iff $\mathbf{F}_1$ has full row rank, we have

$$\begin{aligned} P_1 &\geq \Pr_{\mathbf{F}_1 \xleftarrow{\$} \mathbb{Z}_2^{(n-1)\times(n+t_1)}} [\mathbf{F}_1 \text{ is invertible}] \\ &= \left(1-2^{-(n+t_1)}\right)\left(1-2^{-(n+t_1-1)}\right)\cdots\left(1-2^{-(t_1+2)}\right) > 1-2^{-(t_1+1)}. \end{aligned}$$

Lemma 5.4 (Theorem 15 in [RS62])**.** *For all integer $q \geq 3$,*

$$\frac{\varphi(q)}{q} \geq \frac{1}{e^{\gamma}\cdot\ln\ln q + \frac{3}{\ln\ln q}},$$

where $\gamma = 0.577\cdots$ is the Euler-Mascheroni constant.

The lower bound of P_2 is just a success probability amplification by paralleled sampling:

$$P_2 = 1 - \left(1 - \Pr_{\mathbf{u}_n \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_n \mid \mathsf{E}_{n-1}]\right)^{t_2 \ln\ln q} = 1 - \left(1 - \frac{\varphi(q)}{q}\right)^{t_2 \ln\ln q} \geq 1 - \exp\left(-\frac{\varphi(q)}{q} \cdot t_2 \ln\ln q\right).$$

For $q \geq 25$,

$$\frac{\varphi(q)}{q} \cdot t_2 \ln\ln q \geq t_2 \cdot \frac{\ln\ln q}{e^{\lambda} \cdot \ln\ln q + \frac{3}{\ln\ln q}} > \frac{t_2}{4}$$

Therefore, $P_2 > 1 - e^{-t_2/4}$, yielding that

$$\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q} \leq 1 - P_1 P_2 \leq 2^{-(t_1+1)} + e^{-t_2/4},$$

which completes the proof. □

Remark 5.5. *In Theorem 5.2, if we require the probability $\varepsilon_{\mathsf{non\text{-}inv}}^{n,m',q}$ to be negligible in λ, we need at least $m' \geq n + \omega(\log\lambda \cdot \ln\ln q)$ asymptotically. In fact, the bound $m' \geq n + \omega(\log\lambda \cdot \ln\ln q)$ is asymptotically tightest for general modulus q, since the probability $\Pr_{\mathbf{u}_n}[\mathsf{E}_n \mid \mathsf{E}_{n-1}]$ is exactly $\varphi(q)/q$, then if we already have $n-1$ linearly independent vectors from $\mathbb{Z}_q^n$, we must sample another $\omega(\log\lambda) \cdot \frac{q}{\varphi(q)}$ vectors to overwhelmingly obtain a valid $\mathbf{u}_n$. Also, [Rib89, Chapter 4] shows that there exists infinite number of integer q such that $\varphi(q)/q < e^{-\gamma} \cdot 1/\log\log q$, i.e., these q satisfy that*

$$\frac{1}{e^{\gamma} \cdot \ln\ln q + \frac{3}{\ln\ln q}} \leq \frac{\varphi(q)}{q} \leq \frac{1}{e^{\gamma} \cdot \ln\ln q}.$$

On the other hand, the term $\frac{3}{\ln\ln q}$ is with $o(1)$ order. This means that, for these q, $O(\frac{1}{\ln\ln q})$ is the asymptotically tightest lower bound of $\varphi(q)/q$. Furthermore, it needs at least $\omega(\log\lambda \cdot \ln\ln q)$ independent samples to complete sampling the last vector $\mathbf{u}_n$ for these q. This shows that tightness of the bound $m' \geq n + \omega(\log\lambda \cdot \ln\ln q)$ for general modulus q.

Remark 5.6. *Theorem 5.2 provides a tighter analysis of the probability of uniformly random matrices over $\mathbb{Z}_q^{n\times m}$ having full-rank invertible submatrices (compared to previous analysis in [ACPS09, BLP+13]), thus it can improve the reduction from* HNFLWE *to* LWE *in [ACPS09] and [BLP+13, Lemma 2.12]. In [ACPS09], Applebaum et al. gives a reduction from $\mathsf{LWE}_{n,n^2+k,q,\chi}$ to $\mathsf{HNFLWE}_{n,k,q,\chi}$ for $q = p^e$ as a power of prime and any k, since they need n^2 uniformly random samples from $\mathbb{Z}_q^n$ to create a invertible matrix in $\mathbb{Z}_q^{n\times n}$. Our new results stated in Theorem 5.2 make improvements on (1) generalizing their reduction to arbitrary modulus q, (2) requiring less samples (from n^2 to $n + \omega(\log\lambda \cdot \ln\ln q)$), resulting a reduction from $\mathsf{LWE}_{n,m'+k,q,\chi}$ to $\mathsf{HNFLWE}_{n,k,q,\chi}$ for $m' = n + \omega(\log\lambda \cdot \ln\ln q)$ with arbitrary modulus q.*

Remark 5.7. *In [MM11, MS23], Micciancio et al. proposed a reduction from search-$\mathsf{HNFLWE}_{n,m,q,\chi}$ assumption to the known-norm decision-$\mathsf{HNFLWE}_{n,m,q,\chi}$, which is the decision version of $\mathsf{HNFLWE}_{n,m,q,\chi}$ with leakage $\|\boldsymbol{s}\|^2 + \|\boldsymbol{e}\|^2$. Theorem 5.2 mends a gap in their reduction [MS23, Lemma 20, 21]. Their reduction requires $\varepsilon_{\mathsf{non\text{-}inv}}^{m,m+n,q}$ to be $1 - \mathsf{negl}(\lambda)$. To the best of our knowledge, the previous tightest estimation of $\varepsilon_{\mathsf{non-inv}}^{m,m+n,q}$ is from Brakerski et al. [BLP+13, Claim 2.13], which requires $n \geq 4m + \omega(\log\lambda) \cdot \ln\ln q$. Thus the previous techniques set an unsatisfactory constraint on the number of samples in the* LWE *setting and this requirement cannot support the parameter choices of the threshold public key encryption scheme in [MS23] which suggests $m = n$ and general modulus q. Our Theorem 5.2 mends this gap, and make their scheme safe and*

*sound. Furthermore, combined the reduction framework from [MM11, MS23] with Theorem 5.2, we can obtain a reduction from the search-*HNFLWE *to the decision-*HNFLWE *with a polynomial-sized leakage on the secret and error.*

Remark 5.8. *In [BD20a], authors give an upper bound for the probability of non-existance of an invertible column-submatrix from a uniform matrix* $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m'}$ *with arbitrary modulus q, which is* $2^{n-m'}\log q$*. However, we find that their analysis has a minor technical flaw, which is that the statement "a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *has an invertible column-submatrix modulo q iff it has an invertible column-submatrix modulo all prime factors* p_i *of q" [BD20a] is not correct. Take* $q = 6$ *and* $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \end{pmatrix}$ *as an example. The column-submatrix* $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ *is invertible modulo 3 and* $\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ *is invertible modulo 2, while there does not exist an invertible column-submatrix in* $\mathbf{A}$*. We do not claim any new results for the case when q is a power of a prime, but this example illustrates that distinguishing invertibility from non-singularity for matrix* $\mathbf{A}$ *and general modulus q is essential. This observation is also explicitly stated in Appendix A.2 in [BJRW23].*

Remark 5.9. *Our analysis for the invertibility of* $\mathbb{Z}_q^{n\times m'}$ *in Theorem 5.2 is targeted at coprime q, in which* $\mathbb{Z}_q$ *is not a field any more. This technique can be adapted to the ring case, which is to estimate the probability of invertibility of uniform matrix over* $R_p^{k\times(k+\ell)}$*, since* R_p *is mostly not a field and has factor decomposition into many prime ideals like* $\mathbb{Z}_q$*. Take p prime and completely splitting* R_p *as an example, similarly to Theorem 5.2, the ideal factor decomposition of* R_p *is* $R_p = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$ *where n is the dimension of ring R, and the event* E_i *for* $i \in [k]$ *is defined similarly. We can also prove that* $\Pr_{\boldsymbol{u}_i \xleftarrow{\$} R_p^k}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] = \left(1 - p^{-(k+1-i)}\right)^n \geq 1 - np^{-(k+1-i)}$ *for* $i \in [k]$*. As long as* $p \geq n \cdot \lambda$*, we can obtain* $\Pr[\mathsf{E}_i \mid \mathsf{E}_{i-1}] \geq 1 - \lambda^{-(k+1-i)}$*, then we can use our event transformation technique to prove that*

$$\Pr_{\mathbf{A} \xleftarrow{\$} R_p^{k\times(k+\ell)}}[\mathbf{A} \textit{ is invertible}] \geq (1-\lambda^{-(k+\ell)})\cdots(1-\lambda^{-(\ell+1)}) \geq 1 - \lambda^{-\ell}.$$

5.2 Construction of Compact Lattice Trapdoor

In this part, we show our modifications to the lattice trapdoor algorithm proposed by Micciancio and Peikert [MP12]. Particularly, we similarly set $\mathbf{A} = [\bar{\mathbf{A}} | \bar{\mathbf{A}}\mathbf{R} + \mathbf{G}] \in \mathbb{Z}_q^{n\times m}$ where $\bar{\mathbf{A}} \in \mathbb{Z}_q^{n\times m'}$ is uniformly random and $\mathbf{R}$ follows discrete Gaussian, and show the pseudorandomness of $\bar{\mathbf{A}}\mathbf{R}$ based on the hardness of LWE with Hermite Normal Form under arbitrary modulus q with almost optimal ratio $\frac{m'}{n} = O(1)$ and $\frac{m}{n} = O(1)$.

Before presenting the reduction, we first introduce an polynomial-time algorithm ExInvMat involved in it, which takes an input as a matrix $\mathbf{A}$ in $\mathbb{Z}_q^{n\times m'}$, and outputs n linearly independent column vectors in $\mathbf{A} \in \mathbb{Z}_q^{n\times m'}$ (which forms a corresponding invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$ in definition 5.1) for invertible $\mathbf{A}$ and aborts for non-invertible $\mathbf{A}$. Specifically, the algorithm is as follows:

$\mathsf{ExInvMat}(\mathbf{A})$: On input a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m'}$, this algorithm runs in steps:

1. Split $\mathbf{A}$ as m' column vectors $\{\mathbf{a}_i\}_{1\leq i\leq m'}$ from $\mathbb{Z}_q^n$.
2. Initialize a vector list $\mathbf{H} = \emptyset$ and a register $r = 1$.
3. Check whether $\mathbf{a}_r \in (\mathbb{Z}_q^n)^*$, and vectors from $\mathbf{H} \cup \{\mathbf{a}_r\}$ are linearly independent. If so, add $\mathbf{a}_r$ to $\mathbf{H}$.
4. Let $r \leftarrow r + 1$. Abort if $r > m'$.

   If $|\mathbf{H}| = n$, return $\mathbf{H}$; Otherwise, go to step 3.

This algorithm is a PPT algorithm, as the most complex steps 3 can be done within probabilistic polynomial time. On the other hand, if the input matrix $\mathbf{A}$ is uniformly at random and $m' \geq n + \omega(\log\lambda \cdot \ln\ln q)$, this algorithm will finally return a matrix $\mathbf{H}$ with overwhelming probability.

Based on this and the reduction from [MS23, Lemma 20], we have the following reduction.

Lemma 5.10. *Let λ be a security parameter and let m, n, q be lattice parameters such that q is any integer modulus and $n \geq \omega(\log\lambda \cdot \ln\ln q)$. Let χ be β-bounded distribution over $\mathbb{Z}_q$. Sample $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times(m+n)}$, $\mathbf{r} \leftarrow \chi^{m+n}$ and $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_q^m$. Under the hardness of $\mathsf{HNFLWE}_{n,m,q,\chi}$, the distribution $(\mathbf{A}, \mathbf{Ar})$ is computationally indistinguishable from the distribution $(\mathbf{A}, \mathbf{a})$, i.e.*

$$\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{pse},\mathcal{A}}(\lambda) := \left|\Pr[\mathcal{A}(1^\lambda, \mathbf{A}, \mathbf{Ar}) = 1] - \Pr[\mathcal{A}(1^\lambda, \mathbf{A}, \mathbf{a}) = 1]\right|$$

is negligible for all PPT $\mathcal{A}$.

Proof. This reduction follows similar steps as Lemma 20 [MS23] except that our new analysis in Theorem 5.2 makes the proof strategy sound.

Let $(\mathbf{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ be the input from $\mathsf{HNFLWE}_{n,m,q,\chi}$ challenger. Let $\mathbf{U}$ be a uniform invertible matrix from $\mathbb{Z}_q^{m\times m}$ and $\mathbf{P}$ be a random permutation matrix from $\mathbb{Z}^{(m+n)\times(m+n)}$. We set $\mathbf{B} = \mathbf{U}[\mathbf{A} \mid \mathbf{I}_m]\mathbf{P} \in \mathbb{Z}_q^{m\times(m+n)}$ and $\boldsymbol{b}' = \mathbf{U}\boldsymbol{b}$, then output $(\mathbf{B}, \boldsymbol{b}')$.

Since $\mathbf{A}$ is uniform at random and $\mathbf{U}$ is invertible, then $\mathbf{UA}$ is marginally uniform at random regardless the choice of $\mathbf{U}$. Then $\mathbf{U}[\mathbf{A} \mid \mathbf{I}_m]$ is uniform at random given the last m columns forming an invertible matrix. Therefore, by randomly permuting the columns of $\mathbf{U}[\mathbf{A} \mid \mathbf{I}_m]$, $\mathbf{B}$ follows a uniform distribution conditioned on that there exist m column vectors to be an invertible matrix. From our new analysis in Theorem 5.2 and $n \geq \omega(\log\lambda \cdot \ln\ln q)$, such $\mathbf{B}$ is uniform at random over $\mathbb{Z}_q^{m\times(m+n)}$.

If the input $(\mathbf{A}, \boldsymbol{b} = \mathbf{A}\cdot\boldsymbol{s} + \boldsymbol{e})$ are LWE samples in Hermite Normal Form where $\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix} \leftarrow \chi^{m+n}$, then the output can be written as $(\mathbf{B}, \boldsymbol{b}' = \mathbf{Br})$ where $\mathbf{B}$ is statistically closed to uniform distribution and $\mathbf{r} = \mathbf{P}^{-1}\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}$ follows χ^{m+n} marginally. If the input $(\mathbf{A}, \boldsymbol{b})$ are uniform samples, then the output $(\mathbf{B}, \boldsymbol{b}' = \mathbf{U}\boldsymbol{b})$ are statistically closed to uniform samples due to the invertibility of $\mathbf{U}$. This completes the proof.

□

Next, we describe our compact lattice trapdoor based on the pseudorandomness of HNFLWE samples. We will use definitions of gadget matrix and trapdoor introduced by [MP12, GMP19].

Gadget Matrix. Let m, n, b, q, k be positive integers such that $k = \lceil \log_b q \rceil$ and $m = O(nk)$. Define the gadget vector based on b be $\mathbf{g} = (1, b, b^2, \cdots, b^{k-1})^\top \in \mathbb{Z}_q^k$ and the corresponding gadget matrix $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{nk\times n}$.

Lattice Trapdoors. Let m, n, b, q, k be positive integers with same relationship above. A gadget trapdoor for a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ is a matrix $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{kn\times m}$ such that $\mathbf{T}_\mathbf{A} \cdot \mathbf{A} = \mathbf{G}$. We define a gadget trapdoor is *compact* if k is constant and $m = O(n)$.

Theorem 5.11 (Compact Lattice Trapdoor)**.** *Let m, n, b, q, k be positive integer parameters, χ be a β-bounded distribution over $\mathbb{Z}_q$. Under the hardness assumption of $\mathsf{HNFLWE}_{n,n,q,\chi}$, then there exist efficient algorithms with the following syntax:*

- $\mathsf{TrapGen}(1^n, q, b)$*: Given a dimension n, a modulus q and a gadget base b, the trapdoor generation algorithm returns a compact matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ with a gadget trapdoor $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{kn\times m}$ where $k = \lceil \log_b q \rceil$*

is a constant and $m = O(n)$. We require that the trapdoor $\mathbf{T_A}$ is small and the marginal distribution of $\mathbf{A}$ is computationally indistinguishable from $U(\mathbb{Z}_q^{m\times n})$.

- $\mathsf{LWEInvert}(\mathbf{A}, \mathbf{c}, \mathbf{T_A})$*: Given m* LWE *samples $(\mathbf{A}, \mathbf{c}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and the gadget trapdoor $\mathbf{T_A}$, the* LWE *inversion algorithm returns the secret $s \in \mathbb{Z}_q^n$ such that $\mathbf{c} = \mathbf{A}\cdot s + \mathbf{e}$ for some error $\mathbf{e} \in \mathbb{Z}_q^m$. If $\|\mathbf{e}\|_\infty \le \frac{q}{2(b+1)\|\mathbf{T_A}\|_\infty}$, then this algorithm recovers the secret $\mathbf{s}$ successfully.*

- $\mathsf{LWRInvert}(\mathbf{A}, \mathbf{c}, \mathbf{T_A})$*: Given m* LWR *samples $(\mathbf{A}, \mathbf{c}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_p^m$ and the gadget trapdoor $\mathbf{T_A}$, the* LWR *inversion algorithm returns the secret $s \in \mathbb{Z}_q^n$ such that $\mathbf{c} = \lfloor \mathbf{A}\cdot s \rceil_p$. If $p \ge 2(b+1)\|\mathbf{T_A}\|_\infty$, then the algorithm returns $\mathbf{s}$ successfully.*

In order to let our LWEInvert algorithm work and compute optimal parameters relationship, we need the following *LWE gadget decoding* algorithm [GMP19].

Lemma 5.12 ([GMP19])**.** *For any modulus q and gadget base b, there exists a* poly*-time algorithm* $\mathsf{DecodeG}(\mathbf{c})$ *which takes $\mathbf{c} \in \mathbb{Z}_q^{kn}$ as an input and returns the secret $\mathbf{s} \in \mathbb{Z}_q^n$ such that $\mathbf{c} = \mathbf{G}\cdot s + \mathbf{e}$ for some error vector $\mathbf{e} \in \mathbb{Z}_q^{kn}$ if $\|\mathbf{e}\|_\infty \le \frac{q}{2(b+1)}$.*

Next we instantiate algorithms of our lattice trapdoor in theorem 5.11.

- $\mathsf{TrapGen}(1^n, q, b)$: Let $m' = 2n$. Sample $\mathbf{A}_0 \xleftarrow{\$} \mathbb{Z}_q^{m'\times n}$, and $\mathbf{R} \leftarrow \chi^{kn\times m'}$ and compute $\mathbf{A}_1 \leftarrow \mathbf{R}\cdot\mathbf{A}_0 - \mathbf{G}$. Output the public compact matrix $\mathbf{A} = \begin{pmatrix}\mathbf{A}_0^\top & \mathbf{A}_1^\top\end{pmatrix}^\top$ and its trapdoor $\mathbf{T_A} = \begin{pmatrix}\mathbf{R} & -\mathbf{I}_{kn}\end{pmatrix}$.

- $\mathsf{LWEInvert}(\mathbf{A}, \mathbf{c}, \mathbf{T_A})$: Output $\mathsf{DecodeG}(\mathbf{T_A}\cdot\mathbf{c})$.

- $\mathsf{LWRInvert}(\mathbf{A}, \mathbf{c}, \mathbf{T_A})$ [AKPW13]: First we transform the LWR sample $\mathbf{A}, \mathbf{c} = \lfloor \mathbf{A}\cdot s \rceil_p$ to LWE sample $(\mathbf{A}, \mathbf{c}' = \mathbf{A}\cdot s + \mathbf{e}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ for some error $\mathbf{e}$ by $\mathbf{c}' = \left\lfloor \frac{q}{p}\mathbf{c} \right\rceil$. Then output $\mathsf{DecodeG}(\mathbf{T_A}\cdot\mathbf{c}')$.

Lemma 5.13. *Let $m = (k+2)n$. Assuming the hardness of* $\mathsf{HNFLWE}_{n,n,q,\chi}$*,* TrapGen *generates a valid lattice trapdoor pair $(\mathbf{A}, \mathbf{T_A})$ satisfying $\mathbf{T_A}\cdot\mathbf{A} = \mathbf{G}$, $\|\mathbf{T_A}\|_\infty \le 2n\beta + 1$ overwhelmingly, and the distribution of $\mathbf{A}$ is computationally indistinguishable from $U(\mathbb{Z}_q^{m\times n})$.*

Proof of Lemma 5.13. It is easy to verify the correctness $\mathbf{T_A}\cdot\mathbf{A} = \mathbf{G}$. The pseudorandomness of $\mathbf{A}$ is directly based on Lemma 5.10. For the upper bound of the trapdoor's quality, since $\mathbf{R} \leftarrow \chi^{kn\times 2n}$, with overwhelming probability we have

$$\|\mathbf{T_A}\|_\infty = \|\mathbf{R}\|_\infty + 1 \le 2n\beta + 1.$$

□

Proof of Theorem 5.11. We prove the three algorithms TrapGen, LWEInvert and LWRInvert listed in Section 5.2 satisfy the properties.

From lemma 5.13, proof is done for TrapGen.

For the LWE samples $(\mathbf{A}, \mathbf{c} = \mathbf{A}\cdot s + \mathbf{e})$, we compute

$$\mathbf{T_A}\cdot\mathbf{c} = \mathbf{G}\cdot s + \mathbf{T_A}\cdot\mathbf{e}.$$

Note that $\|\mathbf{T_A}\cdot\mathbf{e}\|_\infty \le \|\mathbf{T_A}\|_\infty \cdot \|\mathbf{e}\|_\infty$. With lemma 5.12, we can successfully output the secret $\mathbf{s}$ from $\mathsf{DecodeG}(\mathbf{T_A}\cdot\mathbf{c})$ if the error norm $\|\mathbf{e}\| \le \frac{q}{2(b+1)\|\mathbf{T_A}\|_\infty}$.

With LWR samples $(\mathbf{A}, \mathbf{c} = \lceil \mathbf{A} \cdot \boldsymbol{s} \rfloor_p)$, the algorithm $\mathsf{LWRInvert}$ first transform c to the form of LWE samples

$$\mathbf{c}' = \left\lceil \frac{q}{p} \cdot \mathbf{c} \right\rfloor = \left\lceil \frac{q}{p} \cdot \left\lceil \frac{p}{q} \cdot \mathbf{A} \cdot \boldsymbol{s} \right\rfloor \right\rfloor = \left\lceil \frac{q}{p} \cdot \left(\frac{p}{q} \cdot \mathbf{A} \cdot \boldsymbol{s} + \mathbf{e}' \right) \right\rfloor = \mathbf{A} \cdot \boldsymbol{s} + \mathbf{e}$$

where $\mathbf{e}' \in (-1/2, 1/2]^m$ and $\mathbf{e} = \lceil (q/p)\mathbf{e}' \rfloor = (q/p)\mathbf{e}' + \mathbf{e}''$ for some $\mathbf{e}'' = (-1/2, 1/2]^m$. Hence $\|\mathbf{e}\|_\infty \leq (q/p + 1)/2 < q/p$. Therefore, as long as $p \geq 2(b+1)\|\mathbf{T}_\mathbf{A}\|_\infty$, the error norm $\|\mathbf{e}\|_\infty < \frac{q}{2(b+1)\|\mathbf{T}_\mathbf{A}\|_\infty}$ then $\mathsf{DecodeG}(\mathbf{T}_\mathbf{A} \cdot \mathbf{c}')$ recovers $\boldsymbol{s}$ successfully. □

5.3 Construction of Compact Lossy Trapdoor Functions

Then, we apply our compact gadget trapdoor to the construction of lossy trapdoor functions. We adopt the LTF construction from [AKPW13] while we make modifications to parameters. First, based on our security reduction for pseudorandomness of entropic LWR, if the secret $\boldsymbol{s}$ is taken from some entropic distributions, we remove the limitations on the bound of this entropic domain. Second, for the case $\mathcal{S}$ covers $\mathbb{Z}_q^n$, we apply the compact trapdoor algorithm to achieve the constant expansion property.

Construction 5.14. *Let λ be a security parameter, $n, m, q, p = \mathsf{poly}(\lambda)$ be integer parameters. Let b be a gadget base and χ be a β-bounded distribution over $\mathbb{Z}_q$. Let $\mathcal{S}$ be a entropic distribution over $\mathbb{Z}_q^n$ and define the range set as $\mathcal{Y} = \mathbb{Z}_p^m$.*

- $\mathsf{LTF.IGen}(1^\lambda)$: Sample $(\mathbf{A}, \mathbf{T}_\mathbf{A}) \leftarrow \mathsf{TrapGen}(1^n, q, b)$. Output $\mathsf{ek} = \mathbf{A}$ and $\mathsf{ik} = \mathbf{T}_\mathbf{A}$.
- $\mathsf{LTF.LGen}(1^\lambda)$: Sample $\mathbf{A} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$. Output $\mathsf{ek}' = \mathbf{A}$.
- $\mathsf{LTF.Eval}(\mathsf{ek}, \boldsymbol{s})$: Input $\mathsf{ek} = \mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and a $\boldsymbol{s} \in \mathbb{Z}_q^n$, output $\lfloor \mathbf{A}\boldsymbol{s} \rceil_p$.
- $\mathsf{LTF.Invert}(\mathsf{ik}, \boldsymbol{y})$: Input the LWR samples $(\mathbf{A}, \boldsymbol{y} = \lfloor \mathbf{A}\boldsymbol{s} \rceil_p)$ and the gadget trapdoor $\mathbf{T}_\mathbf{A}$, use LWR inversion algorithm to output $\mathsf{LWRInvert}(\mathbf{T}_\mathbf{A}, \mathbf{A}, \boldsymbol{y})$.

Then we state that our LTF is a valid and secure lossy trapdoor function .

Theorem 5.15. *Let λ be the security parameter. Let $q > p^* \geq nmp\beta$, $p \geq 2(b+1)(2n\beta+1)$, $k = \lceil \log_b q \rceil = O(1)$ be a constant and $m = (k+2)n$. The consturction $\mathsf{LTF} = (\mathsf{LTF.IGen}, \mathsf{LTF.LGen}, \mathsf{LTF.Eval}, \mathsf{LTF.Invert})$ is an l-lossy and constant-expansion LTF under the hardness of $\mathsf{LWE}_{\ell,m,p,\chi}$ and $\mathsf{HNFLWE}_{n,n,q,\chi}$ for $l = (\ell + \lambda)\log q + n \log p^*$.*

Proof. We separate the proof of Theorem 5.15 into several sub-lemmas and each lemma refers to a property of LTF.

Lemma 5.16 (Constant Expansion)**.** *Let $m = (k+2)n$ and $k = \lceil \log_b q \rceil$ is a constant. If the preimage distribution $\mathcal{S}$ covers $U(\mathbb{Z}_q^n)$, our LTF construction has $O(1)$ expansion.*

Proof. For all $\mathbf{s} \in \mathbb{Z}_q^n$ and (injective or lossy) evaluation key $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, we obtain the image $\boldsymbol{y} = \lfloor \mathbf{A} \cdot \mathbf{s} \rceil_p \in \mathbb{Z}_p^m$. Therefore, we compute the expansion as

$$\eta = \frac{m \cdot \log p}{n \cdot \log q} = O(1).$$

□

Lemma 5.17 (Correctness)**.** *If $p \geq 2(b+1)(2n\beta+1)$ the above construction has overwhelming probability to inverse correctly in the injective mode.*

Proof. This proof is directly from constraints on upper bound of $\|\mathbf{T_A}\|_\infty$ from lemma 5.13 and correctness of LWRInvert from theorem 5.11. □

Lemma 5.18 (l-Lossiness)**.** *For parameters restriction $q > p^* > nmp\beta$, our* LTF *construction has l-lossiness where $l = (\ell + \lambda)\log q + n\log p^*$.*

Lemma 5.19 (Key Indistinguishability)**.** *Let $m = (k+2)n$. Our* LTF *construction achieves key indistinguishability assuming hardness of* $\mathsf{HNFLWE}_{n,n,q,\chi}$ *and* $\mathsf{LWE}_{\ell,m,q,\chi}$.

Proof. From the theorem 5.11, with the assumption of $\mathsf{HNFLWE}_{n,n,q,\chi}$, the distribution of our injective evaluation key $\mathbf{A}$ is computationally indistinguishable from $U(\mathbb{Z}^{m\times n})$.

From the lemma 4.2, under the assumption of $\mathsf{LWE}_{l,m,q,\chi}$, the distribution of our lossy evaluation key $\mathbf{A}'$ is computationally indistinguishable from $U(\mathbb{Z}^{m\times n})$.

With hybrid arguments, the proof is done. □

□

Our construction of All-But-Many Lossy Trapdoor Function (ABM-LTF) is achieved via the technique in [Hof12, LSSS17], which is put to Appendix A.

6 Hardness of Entropic Ring-LWR

In this section, we consider the hardness of entropic RLWR problem. We first establish the one-way hardness of entropic RLWE, i.e., the entropic search RLWR is hard under appropriate parameters. Next we show that RLWR is also pseudorandom for certain entropic secrets (with small coefficients with respect to some basis).

6.1 One-wayness of Entropic RLWR

The main result in this part is adopted from the reduction of search RLWE to search RLWR in [LW20], i.e., we can show a reduction from search entropic RLWE to search entropic RLWR by making use of RD tool. Then, combine with the existing hardness result of search entropic RLWE in Section 2.10, we obtain the one-way hardness of entropic RLWR from the hardness of DSPR and RLWE.

We use $U_\beta(\mathbf{B})$ to denote the distribution over R_q that each coefficient with respect to the basis $\mathbf{B}$ over R is sampled uniformly at random in the interval $[-\beta, \beta]$, and we have the following theorem.

Theorem 6.1 ($\mathsf{ent\text{-}RLWE}_{\ell,q,\chi,\mathcal{S}}$ to $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}}$)**.** *Let $q \geq p \geq 2, n, \ell, B$ be positive integers such that $q \geq 18pB\ell n$, R be a ring of integers of a number field K with degree n, $\mathbf{B}$ be a basis of R. Let χ be a B-bounded distribution over R with respect to basis $\mathbf{B}$, $\mathcal{S}$ be a distribution over R_q^*. Then there exists a poly-time reduction from* $\mathsf{ent\text{-}RLWE}_{\ell,q,\chi,\mathcal{S}}$ *to* $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}}$

Proof. Set $\beta = 2B$. Then the reduction can be obtained by the following two steps:

$$\mathsf{ent\text{-}RLWE}_{\ell,q,\chi,\mathcal{S}} \xrightarrow{(1)} \mathsf{ent\text{-}RLWE}_{\ell,q,\chi+U_\beta(\mathbf{B}),\mathcal{S}} \xrightarrow{(2)} \mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}}.$$

The first reduction is straight-forward: given ℓ samples $(a_i, b_i) \in R_q \times R_q$ where $s \xleftarrow{\$} \mathcal{S}$, the reduction just adds independent samples from $U_\beta(\mathbf{B})$ to each b_i of the basis $\mathbf{B}$. It is easy to see the reduction maps the uniformly random distribution to itself, and $A_{s,\chi}$ to $A_{s,\chi+U_\beta}$, concluding the analysis of this part.

For the second reduction, we can bound the RD between samples from the two distributions. Thus, a solver of RLWR (as is) can be used to solve the Ring-LWE with the specified parameters.

Let $\mathcal{X}_s$ be the distribution of a single ent-$\mathsf{RLWR}_{q,p,\mathbf{B},\mathcal{S}}$ sample, and let $\mathcal{Y}_s$ be that of a single rounded $\mathsf{RLWE}_{q,\chi+U_\beta,\mathcal{S}}$ sample under basis $\mathbf{B}$. By our setting of parameters $\beta = 2B$, the coefficients of $e \leftarrow \chi + U_\beta$ with respect to $\mathbf{B}$ are B'-bounded, where $B' = 3B$. By the definition of Rényi divergence,

$$\begin{aligned}\mathsf{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s) &= E_{a \leftarrow R_q} \frac{\Pr\left(\mathcal{X}_s = (a, \lfloor a \cdot s \rceil_{\mathbf{B},p})\right)}{\Pr\left(\mathcal{Y}_s = (a, \lfloor a \cdot s \rceil_{\mathbf{B},p})\right)} \\ &= E_{a \leftarrow R_q} \frac{1}{\Pr_{e \leftarrow \chi+U_\beta}(\lfloor a \cdot s + e \rceil_{\mathbf{B},p} = \lfloor a \cdot s \rceil_{\mathbf{B},p})}.\end{aligned}$$

Next we define the set

$$\mathsf{border}_{q,p}(B') = \left\{ x \in \mathbb{Z}_q : x - \frac{q}{p}\left(\lfloor x \rceil_p - \frac{1}{2}\right) < B' \text{ or } \frac{q}{p}\left(\lfloor x \rceil_p + \frac{1}{2}\right) - x < B' \right\}.$$

For any $t \in \{0, \cdots, n\}$, we define the set $\mathsf{BAD}_{s,t} = \left\{ a \in R_q : |\{i \in [n], (a \cdot s)_i \in \mathsf{border}_{q,p}(B')\}| = t \right\}$, where $(a \cdot s)_i$ is the ith coefficient of $a \cdot s$ with respect to the basis $\mathbf{B}$. Fix t and $a \in \mathsf{BAD}_{s,t}$, and below we do a case analysis:

- For any $i \in [n]$ such that $(a \cdot s)_i \notin \mathsf{border}_{q,p}(B')$, we have
$$\Pr\left[\lfloor (a \cdot s)_i + e_i \rceil_{\mathbf{B},p} = \lfloor (a \cdot s)_i \rceil_{\mathbf{B},p}\right] = 1.$$
- For any $i \in [n]$ such that $(a \cdot s)_i \in \mathsf{border}_{q,p}(B')$, the event $\lfloor (a \cdot s)_i + e_i \rceil_{\mathbf{B},p} = \lfloor (a \cdot s)_i \rceil_{\mathbf{B},p}$ holds at least in one of the two cases: (1) $e_i \in [-B', \cdots, 0]$ or (2) $e_i \in [0, \cdots, B']$.

Even though the coefficients of e (with respect to $\mathbf{B}$) might not be independent, and thus bounding $\Pr_{e \leftarrow \chi+U_\beta}\left(\lfloor a \cdot s + e \rceil_{\mathbf{B},p} = \lfloor a \cdot s \rceil_{\mathbf{B},p}\right)$ is not straight-forward. To tackle this, we decompose $e = e' + e''$ where $e' \leftarrow \chi$ and $e'' \leftarrow U_\beta(\mathbf{B})$, and note that the coefficients of e'' dominates those of e' (as $\beta = 2B$). More importantly, the coefficients of e with respect to $\mathbf{B}$ become independent of each others (in distribution) when we condition on e'. Since $a \in \mathsf{BAD}_{s,t}$, a has exactly t coefficients in $\mathsf{border}_{q,p}(B')$. Without loss of generality, we assume that the first t coefficients of $(a \cdot s) \in \mathsf{border}_{q,p}(B')$, i.e., $(a \cdot s)_1, \ldots, (a \cdot s)_t$. Next we would like to bound

$$\Pr\left[\lfloor a \cdot s + e \rceil_{\mathbf{B},p} = \lfloor a \cdot s \rceil_{\mathbf{B},p}\right] = \Pr\left[\forall i \in [t]\ \lfloor (a \cdot s)_i + e_i \rceil_{\mathbf{B},p} = \lfloor (a \cdot s)_i \rceil_{\mathbf{B},p}\right].$$

We know that for any $i \in [t]$, the event $\lfloor (a \cdot s)_i + e_i \rceil_{\mathbf{B},p} = \lfloor (a \cdot s)_i \rceil_{\mathbf{B},p}$ happens if $e''_i + e'_i$ falls belong to the correct half. Since e'_i is B bounded and $\beta = 2B$, this happens with probability at least $1/4$ over the choice of e''_i. As the $\{e''_i\}_{i \in [t]}$ are independent, we have

$$\Pr\left[\forall i \in [t]\ \lfloor (a \cdot s)_i + e_i \rceil_{\mathbf{B},p} = \lfloor (a \cdot s)_i \rceil_{\mathbf{B},p}\right] \geq (1/4)^t.$$

On the other hand, $s \in \mathcal{S} \subseteq (R_q)^*$, so $a \cdot s$ is uniformly random over R_q, implying $\Pr[a \in \mathsf{BAD}_{s,t}] \leq \binom{n}{t} \cdot \left(1 - \frac{|\mathsf{border}_{q,p}(B')|}{q}\right)^{n-t} \left(\frac{|\mathsf{border}_{q,p}(B')|}{q}\right)^t$. Conditioning over the event $a \in \mathsf{BAD}_{s,t}$, we have

$$\mathsf{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s) \leq \sum_{t=0}^{n} 4^t \cdot \Pr[a \in \mathsf{BAD}_{s,t}] = \left(1 + \frac{3|\mathsf{border}_{q,p}(B')|}{q}\right)^n.$$

By the definition of RD_2, it is easy to see

$$\mathsf{RD}_2(\mathcal{X}_s^\ell \| \mathcal{Y}_s^\ell) \le \left(1 + \frac{3|\mathsf{border}_{q,p}(B')|}{q}\right)^{\ell n},$$

for ℓ independent samples.

Define the functions $f(\eta) = \frac{\Pr[\mathcal{X}=\eta]}{\sqrt{\Pr[\mathcal{Y}=\eta]}}$, and $g(\eta) = \sqrt{\Pr[\mathcal{Y}=\eta]}$. By the properties of Lemma 2.6 and Cauchy-Schwarz inequality, we have that for any event E, $\Pr[\mathcal{Y}^\ell \in E] \ge \frac{\Pr[\mathcal{X}^\ell \in E]^2}{\mathsf{RD}_2(\mathcal{X}^\ell \| \mathcal{Y}^\ell)}$. Further more, Let E be the event $\{(\boldsymbol{a}, \boldsymbol{b}) : \mathsf{Search}(\boldsymbol{a}, \boldsymbol{b}) = s\}$,

$$\Pr_{\boldsymbol{a},\boldsymbol{e}}\left[\mathsf{Search}(\boldsymbol{a}, \lfloor \boldsymbol{a}\cdot s + \boldsymbol{e}\rceil_{\mathbf{B},p}) = s\right] \ge \frac{\Pr_{\boldsymbol{a}}\left[\mathsf{Search}(\boldsymbol{a}, \lfloor \boldsymbol{a}\cdot s\rceil_{\mathbf{B},p}) = s\right]^2}{\left(1 + \frac{3|\mathsf{border}_{q,p}(B')|}{q}\right)^{\ell n}}.$$

The desired conclusion follows from $|\mathsf{border}_{q,p}(B')| \le 2pB'$ and the parameter settings in the theorem. □

We note that the reduction in Theorem 6.1 is not affected by the entropy requirement of distribution $\mathcal{S}$, i.e., it only requires the samples from $\mathcal{S}$ is invertible over R_q. On the other hand, this reduction is entropy preserving for secret. This nice property enables us to obtain a reduction from DSPR and RLWE to ent-sRLWR by combining the reduction of ent-RLWE in Corollary 2.34.

Corollary 6.2. *Let $q \ge p \ge 2, n, \ell, B$ be positive integers, σ, σ_0, γ be positive real numbers such that n is a power of 2, $\ell \ge 2n\log q + \omega(\log(\lambda))$, $\sigma_0 \ge O(\sigma n \log^2(n)\sqrt{\ell}B)$ and $q \ge 18p\sigma_0\ell n\log(n)$, R be a cyclotomic ring with degree n, $\mathbf{B}$ be a basis of R. Let χ be a B-bounded distribution over R with respect to basis $\mathbf{B}$, $\mathcal{S}$ be a distribution over R_q^* such that $\nu_\sigma(\mathcal{S}) \ge n\log(\gamma\cdot\sqrt{n}\log(n)) + \omega(\log(\lambda))$. Assume that* DSPR *with parameter γ and* RLWE *with noise distribution χ holds, then* ent-sRLWR$_{q,p,\mathbf{B},\ell,\mathcal{S}}$ *is hard.*

6.2 Pseudorandomness of Entropic RLWR

In this part, we proceed to prove that entropic decision RLWR problem is hard for certain entropic secrets. Different from the module case (with module rank greater than 1), one can not apply the randomness extraction procedure to the ring case. Alternatively, we will show a reduction from entropic search RLWR for special entropic secrets to entropic decision RLWR. Combine with the one-way hardness of entropic RLWR in Section 6.1, the pseudorandomness of entropic RLWR is obtained. To be consistent with Corollary 6.2, we consider the cyclotomic ring with power-of-two degree. We use $U_{B_1,B_2}(\mathbf{B})$ to denote the distribution over R_q that with respect to the basis $\mathbf{B}$, the constant coefficient is sampled uniformly at random and independently in the interval $[B_2 - B_1, B_2 + B_1]$ and other coefficients are sampled uniformly at random in the interval $[-B_1, B_1]$, where $0 < B_1 < B_2$ and $B_1 + B_2 < q$, and use $D_{R,\sigma}^{\mathsf{Coeff}(\mathbf{B})}$ to denote the distribution over R that each coefficient with respect to the basis $\mathbf{B}$ over R is sampled according to discrete Gaussian with parameter σ. Then our main theorem of this part is as follow.

Theorem 6.3. *Let $R = \mathbb{Z}[X]/(X^n+1)$ with $n \ge 8$ a power of 2, $q \ge p \ge B_1 + B_2 \ge 2$ be integers such that $p > n$ is a prime, $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ where $g = n/c$ for a constant $c \in \mathbb{Z}$, and $q = p^t$ is a constant power of p. Let $\tau = \mathsf{poly}(n)$ be a polynomial. Let $\mathbf{B} = \{1, X, X^2, \cdots, X^{n-1}\}$ be the power basis of R. Then there exists a reduction from* ent-sRLWR$_{q,p,\mathbf{B},\ell,\mathcal{S}}$ *to* ent-dRLWR$_{q,p,\mathbf{B},\ell',\mathcal{S}'}$*, where $\mathcal{S}$ denotes $U_{B_1,B_2}(\mathbf{B})$ for $B_1 = \frac{\tau}{n}\sqrt{\frac{c\ln n}{n}}$ and $B_2 = \tau$, $\mathcal{S}'$ denotes $D_{R,\sigma}^{\mathsf{Coeff}(\mathbf{B})}$ for $\sigma = O(\tau^2\sqrt{n\log n}p^{\frac{1}{g}})$, $\ell' = gp^c\ell\cdot\mathsf{poly}(1/\varepsilon)$, and ε is the advantage of* ent-dRLWR$_{q,p,\mathbf{B},\ell',\mathcal{S}'}$ *oracle.*

The proof of Theorem 6.3 consists of three reductions following the approach of [LW20]. We summarize the reduction route as follows, and explain the parameters later:

$$\begin{aligned}\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell',\mathcal{S}} &\xrightarrow{6.5} \text{(W)-}\mathfrak{p}_i\text{-}\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}} \xrightarrow{6.8} \text{(W)-}D\text{-}\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}} \\ &\xrightarrow{6.10} \text{(A)-}D\text{-}\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}'} \xrightarrow{6.15} \mathsf{ent\text{-}dRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}'}.\end{aligned}$$

6.2.1 $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell',\mathcal{S}}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$

Definition 6.4 ((W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$)**.** *The worst-case (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\mathcal{S}}$ problem is: given ℓ'' samples from $L_{s,q,p}(R,\mathbf{B})$ for some arbitrary $s \in \mathsf{Supp}(\mathcal{S})$, find $s \bmod \mathfrak{p}_i R^\vee$.*

Then we give our lemma for reduction from $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell',\mathcal{S}}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$.

Lemma 6.5 ($\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell',\mathcal{S}}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$)**.** *For every $i \in \{1,\cdots,g\}$, there exists a deterministic poly-time reduction from $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell',\mathcal{S}}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$, where $\ell' = g\ell''$.*

Proof. To prove this theorem, we will work on an arbitrary $i \in \{1,\cdots,g\}$. The same argument can be extended to all the other i's. Throughout the rest of the poof, we will view i as an arbitrary fixed index.

We first observe a simple fact. For $k \in \{1,\cdots,g\}$, let σ_k be an automorphism that maps $\mathfrak{p}_k$ to $\mathfrak{p}_i$. We know that all these automorphisms exist as $K = \mathbb{Q}[X]/(X^n+1)$ is a Galois extension. Then the reduction proceeds as follow.

- For each $k \in \{1,\cdots,g\}$, the reduction runs through the following steps.
  - Make ℓ'' queries to the oracle $L_{s,q,p}(R,\mathbf{B})$.
  - For each given sample (a,b), transform it to $(\sigma_k(a),\sigma_k(b))$.
  - Send the ℓ'' transformed samples to the $\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ oracle
  - Upon receiving the answer $x \in R/\mathfrak{p}_i R$, store $\sigma_k^{-1}(x) \in R/\mathfrak{p}_k R$.
- Next, the reduction combines all $\{\sigma_k^{-1}(x)\}_{k\in\{1,\cdots,g\}}$ by the Chinese Remainder Theorem. Then it outputs the combined value $s' \in R_p$.

We now show that for each $k \in [g]$, $\sigma_k^{-1}(x) = s \bmod \mathfrak{p}_k R$. To show this, we prove that the distribution of the transformed samples is correctly distributed as the $\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ oracle requires. Particularly, for each $(a,b) \leftarrow L_{s,q,p}(R,\mathbf{B})$, $\sigma_k(a)$ is uniformly random in $\sigma_k(R_q) = R_q$ as σ_k is an automorphism. Furthermore, it's easy to see $\sigma(\mathcal{S}) = \mathcal{S}$, since the effect of σ on $s \in \mathcal{S}$ is just a permutation of the coefficients (up to a sign). Next we would like to show that $\sigma_k(b) = \lfloor \sigma_k(a)\cdot\sigma_k(s)\rceil_{\mathbf{B},p}$. If this holds, then $(\sigma_k(a),\sigma_k(b))$ would be the correct distribution that the $\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ oracle expects, and then the oracle would return $x = \sigma_k(s) \bmod \mathfrak{p}_i R$ (with a non-negligible probability). Thus, we have $\sigma_k^{-1}(x) = s \bmod \mathfrak{p}_k R$. Now we focus on proving $\sigma_k(b) = \lfloor \sigma_k(a)\cdot\sigma_k(s)\rceil_{\mathbf{B},p}$.

We analyze the term $b = \lfloor a\cdot s\rceil_{\mathbf{B},p}$. Without loss of generality, we write $a\cdot s \bmod qR = \sum_{i=0}^{n-1}\alpha_i X^i$ for $\alpha_i \in \mathbb{Z}_q$, $i \in [n]$. When rounding with respect to this basis, we can write $b = \sum_{i=0}^{n-1}\lfloor\alpha_i\rceil_p X^i \in R_p$. By taking the automorphism σ_k, we have $\sigma_k(b) = \sigma_k\Big(\sum_{i=0}^{n-1}\lfloor\alpha_i\rceil_p X^i\Big) = \sum_{i=0}^{n-1}\lfloor\alpha_i\rceil_p\sigma_k(X^i)$. Next we observe that $\sigma_k(a\cdot s \bmod qR) = \sigma_k(a)\cdot\sigma_k(s) \bmod qR$, which is also equal to $\sigma_k\big(\sum_{i=0}^{n-1}\alpha_i X^i\big)$. Then we have $\lfloor\sigma_k(a)\cdot\sigma_k(s)\rceil_{\mathbf{B},p} = \lfloor\sigma_k\big(\sum_{i=0}^{n-1}\alpha_i X^i\big)\rceil_{\mathbf{B},p} = \lfloor\sum_{i=0}^{n-1}\alpha_i\sigma_k(X^i)\rceil_{\mathbf{B},p}$.

On the other hand, we know that σ_k acts as a permutation over the basis (up to a sign), i.e., $\sigma_k(\mathbf{B})$ is equivalent to $\mathbf{B}$ up to a signed permutation. In addition, it holds that $\lfloor -x \rceil = -\lfloor x \rceil$ for rounding function $\lfloor \cdot \rceil$ and any $x \in \mathbb{Z}$. Thus,

$$\lfloor \sigma_k(a) \cdot \sigma_k(s) \rceil_{\mathbf{B},p} = \left\lfloor \sum_{i=1}^{n} \alpha_i \sigma_k(X^i) \right\rceil_{\mathbf{B},p} = \sum_{i=1}^{n} \lfloor \alpha_i \rceil_p \sigma_k(X^i) = \sigma_k(b).$$

Finally, by the Chinese Reminder Theorem, $s \bmod pR$ can be reconstructed from $\{s \bmod \mathfrak{p}_k R\}_{k=1}^{g}$. Since the secret distribution $\mathcal{S}$ has support over $R_\alpha \subseteq R_p$, we have $s = s \bmod pR$. This completes the proof. □

6.2.2 (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ to (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$

Definition 6.6 (Hybrid RLWR distribution)**.** *For $i \in \{1, \cdots, g\}$, $s \in R_p$, we define the distribution $L^i_{s,q,p}(R, \mathbf{B})$ over $R_q \times R_p$ as: sample $(a, b) \leftarrow L_{s,q,p}(R, \mathbf{B})$ and output $(a, b + h)$ where $h \in R_p$ is uniformly random over mod $\mathfrak{p}_j R$ for all $j \le i$, and 0 over mod all the other ideals, i.e., $\mathfrak{p}_j R$'s for $j > i$.*

We note that $L^0_{s,q,p}(R, \mathbf{B})$ is the same as $L_{s,q,p}(R, \mathbf{B})$, $L^g_{s,q,p}(R, \mathbf{B})$ is the uniformly random distribution over $R_q \times R_p$, and the other $L^i_{s,q,p}(R, \mathbf{B})$'s are intermediate hybrids, which will be used via a hybrid argument later.

Definition 6.7 ((W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$)**.** *The worst-case D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ problem is defined as follows: given ℓ samples from $L^j_{s,q,p}(R, \mathbf{B})$ for arbitrary $s \in \mathsf{Supp}(\mathcal{S})$ and $j \in \{i-1, i\}$, determine j.*

Next we present our lemma for reduction from $\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ to (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$.

Lemma 6.8 ((W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ to (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$)**.** *Let $p \mid q$. For any $i \in \{1, \cdots, g\}$, and ideal $\mathfrak{p}_i$ with $N(\mathfrak{p}_i) = p^{n/g} = p^c$ where $c \ge 1$ is a constant integer, there exists a probabilistic polynomial time reduction from (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell'',\mathcal{S}}$ to (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ where $\mathcal{S}$ can be any distribution over R_q, $\ell'' = p^c \ell \cdot \mathsf{poly}(1/\varepsilon)$, and ε is the advantage of the (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ oracle.*

Proof. At a high level, the reduction recovers $s \bmod \mathfrak{p}_i R$ by trying each of its possible values, and uses the (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ oracle to determine which trial is correct. For each trial, the reduction transforms samples from $L_{s,q,p}(R, \mathbf{B})$ so that the resulting samples are distributed according to $L^{i-1}_{s,q,p}(R, \mathbf{B})$ if the trial equal to the value of $s \bmod \mathfrak{p}_i R$, or otherwise, $L^i_{s,q,p}(R, \mathbf{B})$. Then the (W)-$D$-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ oracle can be used to distinguish the two cases, and thus the reduction can determine whether this trial is correct. Since there are $N(\mathfrak{p}_i) = p^c = \mathsf{poly}(n)$ possible values, the reduction's running time is upper bounded by a polynomial. Moreover, the reduction needs to call (W)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}}$ $\mathsf{poly}(1/\varepsilon)$ times in order to get a sufficient confidence, and each call takes ℓ samples. Thus, in total the reduction needs up to $\ell'' = p^c \ell \cdot \mathsf{poly}(1/\varepsilon)$ samples.

Below we just describe the transformation, and note that the other steps of the reduction are trivial (ref. [LPR10]). Given a sample $(a, b) \leftarrow L_{s,q,p}(R, \mathbf{B})$ and a trial value $g \in \psi$, the reduction computes a sample

$$(a', b') = \left(a + \frac{q}{p} v, b + h + vg \right) \in R_q \times R_p,$$

where $v \in R_p$ is sampled according to the distribution that is uniformly random mod $\mathfrak{p}_i R$ and 0 mod all the other $\mathfrak{p}_j R$'s, and $h \in R_p$ is uniformly random mod $\mathfrak{p}_i R$ for all $j < i$, and is $0 \mod \mathfrak{p}_j R$'s for $j \ge i$.

It is clear that a' is uniformly random over R_q because a is uniformly random over R_q. On the other hand, b' can be written as

$$\begin{aligned} b' &= b + h + vg \\ &= \lfloor a \cdot s \rceil_{\mathbf{B},p} + h + vg \\ &= \lfloor a' \cdot s - \frac{q}{p} v \cdot s \rceil_{\mathbf{B},p} + h + vg \\ &= \lfloor a' \cdot s \rceil_{\mathbf{B},p} + h + v(g - s). \end{aligned}$$

If $s \equiv g \bmod \mathfrak{p}_i R$, then by the Chinese Remainder Theorem 2.11, $v(s-g) = 0 \bmod pR$. In this case, (a', b') is distributed according to $L^{i-1}_{s,q,p}(R, \mathbf{B})$. Otherwise if $s \neq g \bmod \mathfrak{p}_i R$, we claim that $v(s-g) \bmod \mathfrak{p}_i R$ is uniformly random over mod $\mathfrak{p}_i R$ and is 0 mod all the other ideals $\mathfrak{p}_j R$'s for $j \neq i$: as $R/\mathfrak{p}_i$ is a field, $v(s-g)$ mod $\mathfrak{p}_i R$ is uniformly random for a random v mod $\mathfrak{p}_i R$, and any $(s-g) \neq 0 \mod \mathfrak{p}_i R$. Therefore, $v(g-s)+h$ is uniformly random mod $\mathfrak{p}_j R$ for all $j \leq i$, and is 0 mod all the remaining $\mathfrak{p}_j R$'s. Thus, the distribution of (a', b') follows $L^{i}_{s,q,p}(R, \mathbf{B})$ in this case, completing the proof. □

6.2.3 (W)-D-$\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}}$ to (A)-D-$\mathsf{RLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$

Definition 6.9 ((A)-D-$\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$)**.** *The average-case D-$\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$ problem is defined as follows: given ℓ samples from $L^{j}_{s,q,p}(R, \mathbf{B})$ for $s \leftarrow \mathcal{S}'$ and $j \in \{i-1, i\}$, determine j.*

For any element $a \in R_q$ and a basis $\mathbf{B}$ of R, we denote $\mathsf{Coeff}_{\mathbf{B}}(a)$ as the coefficient vector of a with respect to $\mathbf{B}$, i.e., $\mathsf{Coeff}_{\mathbf{B}}(a) = (a_0, a_1, \cdot, a_{n-1}) \in \mathbb{Z}_q^{n-1}$ for $a = \sum_{i=1}^{n} a_{i-1} \boldsymbol{b}_i$, where $\mathbf{B} = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$. Similarly, we denote $\mathsf{Rot}_{\mathbf{B}}(a)$ as rotation matrix of a with respect to $\mathbf{B}$, i.e.,

$$\mathsf{Rot}_{\mathbf{B}}(a) = \begin{bmatrix} \mathsf{Coeff}_{\mathbf{B}}(a \cdot \boldsymbol{b}_1 \bmod qR)^\top \\ \mathsf{Coeff}_{\mathbf{B}}(a \cdot \boldsymbol{b}_2 \bmod qR)^\top \\ \vdots \\ \mathsf{Coeff}_{\mathbf{B}}(a \cdot \boldsymbol{b}_n \bmod qR)^\top \end{bmatrix}.$$

It's easy to verify $\mathsf{Coeff}_{\mathbf{B}}(sr) = \mathsf{Coeff}_{\mathbf{B}}(s) \cdot \mathsf{Rot}_{\mathbf{B}}(r) = \mathsf{Coeff}_{\mathbf{B}}(rs) = \mathsf{Coeff}_{\mathbf{B}}(r) \cdot \mathsf{Rot}_{\mathbf{B}}(s)$ for any $s, r \in R_q$.

The following lemma shows a worst-case to average case reduction from the RLWR with secrete distribution $\mathcal{S}$ to the RLWR with $\mathcal{S}_2$, and the measurement RD in the statement denoted as the "Rényi divergence" is defined in Section 2.5.

Lemma 6.10 (Worst-case to average-case)**.** *Let $\mathcal{S}, \mathcal{S}_1, \mathcal{S}_2$ be distributions over R_q. For every $i \in \{1, \cdots, g\}$, if $r \leftarrow \mathcal{S}_1$ is invertible with non-negligible probability, and $\mathsf{RD}_2(\mathsf{Coeff}_{\mathbf{B}}(\mathcal{S}_2) \| \mathsf{Rot}_{\mathbf{B}}(s) \cdot \mathsf{Coeff}_{\mathbf{B}}(\mathcal{S}_1)) \leq \mathsf{poly}(\lambda)$ for any $s \in \mathsf{Supp}(\mathcal{S})$. Then there exists a randomized poly-time reduction from worst-case (W)-D-$\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}}$ to average-case D-$\mathsf{RLWR}^{i}_{q,p,\mathbf{B},\ell,\mathcal{S}_2}$.*

Proof. Given sample $(a, b) \leftarrow L^{i}_{s,q,p}(R, \mathbf{B})$ for arbitrary $s \in \mathsf{Supp}(\mathcal{S})$, the reduction transforms it into $(a', b') = (ar^{-1}, b + h) \in R_q \times R_p$, where $r \leftarrow \mathcal{S}_1$, and $h \in R_q$ is uniformly random mod $\mathfrak{p}_j R$ for all $j \leq \nu$ (where $\nu \leq i$), and 0 over mod all the other ideals. It's clear that a' is uniformly random, since a is uniformly random and r^{-1} is invertible. For the other term, we have $b' = b + h = \lfloor a \cdot s \rceil_{\mathbf{B},p} + h = \lfloor ar^{-1} \cdot rs \rceil_{\mathbf{B},p} + h$. Therefore, for all $s \in R_q$ and $i \in \{1, \cdots, g\}$, this transformation maps $L^{i}_{s,q,p}(R, \mathbf{B})$ to $L^{\max\{\nu, i\}}_{s \cdot \mathcal{S}_1, q, p}(R, \mathbf{B})$.

Formally, the reduction is executed by repeating the following steps a polynomial number of times: Choose an r from $\mathcal{S}_1$, and then estimate the acceptance probability of the oracle on the following two input

distributions: the first is obtained from our input by applying the above transformation with parameters r, and $i-1$; the second is obtained similarly using parameters r, and i. If in any of these polynomial number of attempts a non-negligible difference is observed between the two acceptance probabilities, output "$i-1$"; otherwise output "i".

If the input distribution is $L^i_{s,q,p}(R,\mathbf{B})$, then in each of the attempts, the two distributions on which we estimate the oracle's acceptance probability are exactly the same, and we output "i" with overwhelming probability. If the input distribution is $L^{i-1}_{s,q,p}(R,\mathbf{B})$, we estimate the oracle's acceptance probability on $L^{i-1}_{s\cdot\mathcal{S}_1,q,p}(R,\mathbf{B})$ and $L^{i}_{s\cdot\mathcal{S}_1,q,p}(R,\mathbf{B})$.

Let $B^{i-1}(r)$ and $B^i(r)$ be the two distributions on the sample which our reduction uses as input to the oracle. The average of $B^{i-1}(r)$ over r chosen from $\mathcal{S}_1$, is $L^{i-1}_{s\cdot\mathcal{S}_1,q,p}(R,\mathbf{B})$ and similarly with B^i and L^i.

Let S be the set of all secrets s for which the oracle has a non-negligible difference in acceptance probability on $B^{i-1}(r)$ and $B^i(r)$. By assumption, the measure of S under $\mathcal{S}_2$ is non-negligible. By condition of lemma, the measure of S under $s\cdot\mathcal{S}_1$ is also non-negligible. This finishes the proof. □

According to this lemma, we need to instantiate the distributions $\mathcal{S},\mathcal{S}_1,\mathcal{S}_2$ satisfied the constraints above. The following theorem shows the concrete instantiations that can be applied to our reduction.

Theorem 6.11. *Let $K=\mathbb{Q}(\zeta)$ be m-th cyclotomic number field with m power of 2 and degree $n=m/2$. Let D^n_α and D^n_β be two Gaussian distributions on $\mathbb{R}^n$ with parameters $\alpha,\beta>0$ satisfying $\beta=\tau\alpha$ where $\tau=\tau(n)$ is a polynomial. For all non-zero $s=\sum_{i=0}^{n-1}s_i\cdot\zeta^i$ with fixed coefficient $s_0\in\left[\tau\left(1-\frac{1}{n}\sqrt{\frac{c\ln n}{n}}\right),\tau\left(1+\frac{1}{n}\sqrt{\frac{c\ln n}{n}}\right)\right]$ and $s_i\in\left[-\frac{\tau}{n}\sqrt{\frac{c\ln n}{n}},\frac{\tau}{n}\sqrt{\frac{c\ln n}{n}}\right]$ for $i\in\{1,2,\cdots,n-1\}$, we have $\mathsf{RD}_2(D^n_\beta,\mathsf{Rot}(s)\cdot D^n_\alpha)\le n^{2c+\varepsilon}$ for any constant $\varepsilon>0$.*

Proof. For fixed s, it is obvious that $\mathsf{Rot}(s)\cdot D^n_\alpha$ is exactly $D_{\alpha\mathsf{Rot}(s)}$. In order to compute the RD between two multivariate Gaussian distributions, we first need the following lemma, which gives the RD between two elliptical Gaussian distributions over $\mathbb{R}^n$ with Gaussian parameters $\mathbf{S}_1,\mathbf{S}_2\in\mathbb{R}^{n\times n}$ from [GAL13], .

Lemma 6.12 (Case for Multivariate Gaussian, [GAL13])**.** *For invertible square matrices $\mathbf{S_1},\mathbf{S_2}\in\mathbb{R}^{n\times n}$, let $D_{\mathbf{S}_1}$ and $D_{\mathbf{S}_2}$ be two continuous multivariate Gaussian distributions on $\mathbb{R}^n$ with covariance matrix $\mathbf{S}_1\mathbf{S}_1^\top$ and $\mathbf{S}_2\mathbf{S}_2^\top$. If $2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top$ is positive definite, we have*

$$\mathsf{RD}_2(D_{\mathbf{S}_1},D_{\mathbf{S}_2})=\frac{(\det\mathbf{S}_2)^2}{|\det\mathbf{S}_1|\cdot\sqrt{\det(2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top)}}.$$

Proof. From the definition of Rényi divergence, we can compute that

$$\begin{aligned}
\mathsf{RD}_2\left(D_{\mathbf{S}_1}\|D_{\mathbf{S}_2}\right) &= \int_{\mathbb{R}^n}\left(\frac{\exp\left(-\mathbf{x}^\top\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}\mathbf{x}\right)}{|\det\mathbf{S}_1|}\right)^2\left(\frac{\exp\left(-\mathbf{x}^\top\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}\mathbf{x}\right)}{|\det\mathbf{S}_2|}\right)^{-1}d\mathbf{x}\\
&= \frac{|\det\mathbf{S}_2|}{(\det\mathbf{S}_1)^2}\cdot\int_{\mathbb{R}^n}\exp\left(-\mathbf{x}^\top\left(2\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}-\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}\right)\mathbf{x}\right)d\mathbf{x}\\
&= \frac{|\det\mathbf{S}_2|}{(\det\mathbf{S}_1)^2}\cdot\frac{1}{\sqrt{\det\left(2\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}-\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}\right)}}\\
&= \frac{(\det\mathbf{S}_2)^2}{|\det\mathbf{S}_1|\cdot\sqrt{\det\left(2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top\right)}}.
\end{aligned}\tag{8}$$

The third and fourth equality holds under the fact that

$$2\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}-\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}=\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}\left(2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top\right)\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}$$

and $2\left(\mathbf{S}_1\mathbf{S}_1^\top\right)^{-1}-\left(\mathbf{S}_2\mathbf{S}_2^\top\right)^{-1}$ is positive definite if $2\mathbf{S}_2\mathbf{S}_2^\top-\mathbf{S}_1\mathbf{S}_1^\top$ is positive definite. □

With Lemma 6.12, our next goal is to bound the determinant. Since determinant of each square matrix is equal to the multiplication of n eigenvalues, we need the Gershgorin Circle lemma to bound each eigenvalue.

Lemma 6.13 (Gershgorin Circle [Ger31])**.** *Let $\mathbf{A}=(a_{ij})_{i,j\in[n]}\in\mathbb{C}^{n\times n}$ and $r_i=\sum_{j\neq i}|a_{ij}|$ be the sum of the absolute values of the non-diagonal parts of i-th row for $i\in[n]$. Let $\mathsf{Disk}(a_{ii},r_i)\subset\mathbb{C}$ be the i-th closed disc with center a_{ii} and radius r_i. Then for every eigenvalue $\lambda\in\mathbb{C}$ of $\mathbf{A}$, their exists $i\in[n]$ such that $\lambda\in\mathsf{Disk}(a_{ii},r_i)$.*

We notice that for $s\in R_q$ where R is a cyclotomic ring with power of 2, then $\mathsf{Rot}(s)$ becomes an anti-circulant matrix, indicating that every Gershgorin circle of $\mathsf{Rot}(s)$ is the same which gives a more convenient way to bound each eigenvector:

Corollary 6.14. *Let $s=\sum_{i=0}^{n-1}s_i\cdot\zeta^i\in K_{\mathbb{R}}$ and $\mathbf{S}=\mathsf{Rot}(s)$ be the anti-circulant matrix of the polynomial s. For every eigenvalue $\lambda\in\mathbb{C}$ of $\mathbf{S}$, we have*

$$|s_0|-\sum_{i=1}^{n-1}|s_i|\leq|\lambda|\leq\sum_{i=0}^{n-1}|s_i|.$$

With the foundations above, we give the proof of Theorem 6.11. Denote $\mathbf{S}=\mathsf{Rot}(s)$ as the anti-circulant matrix. We can verify that $\mathbf{S}\mathbf{S}^*=\mathbf{S}^*\mathbf{S}$, hence $\mathbf{S}$ is a normal matrix. Then $\mathbf{S}$ has n eigenvalues $\{\lambda_i\}_{i\in[n]}$ and we obtain the unitary diagonalisation $\mathbf{S}=\mathbf{U}\mathbf{D}\mathbf{U}^*$ where $\mathbf{U}$ is a unitary matrix and $\mathbf{D}=\mathsf{diag}(\lambda_0,\lambda_1,\cdots,\lambda_{n-1})$. Applyling the corollary 6.14, we can restrict the length of each eigenvalue λ_i, $\tau\left(1-\sqrt{\frac{c\ln n}{n}}\right)\leq|\lambda_i|\leq\tau\left(1+\sqrt{\frac{c\ln n}{n}}\right)$. We also notice that $2\alpha^2\mathbf{S}\mathbf{S}^\top-\beta^2\mathbf{I}=\mathbf{U}\left(2\alpha^2\mathbf{D}\mathbf{D}^*-\beta^2\mathbf{I}\right)\mathbf{U}^*$ where $\mathbf{I}$ refers to the n-dimensional identity matrix, so that n eigenvalues of $2\alpha^2\mathbf{S}\mathbf{S}^\top-\beta^2\mathbf{I}$ are exactly $\{2\alpha^2|\lambda_i|^2-\beta^2\}_{i\in[n]}$.

We are also able to verify that $\mathbf{S}$ is invertible and the distribution $\mathbf{S} \cdot D_\alpha^n$ is exactly $D_{\alpha\mathbf{S}}$. Apply the Lemma 6.12 to $\beta\mathbf{I}_n$ and $\alpha\mathbf{S}$, we have

$$\begin{aligned}\mathsf{RD}_2(D_\beta^n \| D_{\alpha\mathbf{S}}) &= \frac{\alpha^{2n}|\det\mathbf{S}|^2}{\beta^n \cdot \sqrt{\det(2\alpha^2\mathbf{S}\mathbf{S}^\top - \beta^2\mathbf{I}_n)}} = \frac{\alpha^{2n}\prod_{i=0}^{n-1}|\lambda_i|^2}{\beta^n \cdot \sqrt{\prod_{i=0}^{n-1}\left(2\alpha^2|\lambda_i|^2 - \beta^2\right)}} \\ &= \frac{\prod_{i=0}^{n-1}|\lambda_i|^2}{\tau^n \cdot \sqrt{\prod_{i=0}^{n-1}(2|\lambda_i|^2 - \tau^2)}} \le \left(\max\left\{\frac{\lambda_{\max}^2}{\tau\sqrt{2\lambda_{\max}^2 - \tau^2}}, \frac{\lambda_{\min}^2}{\tau\sqrt{2\lambda_{\min}^2 - \tau^2}}\right\}\right)^n \end{aligned} \tag{9}$$

where $\lambda_{\max} = \tau\left(1 + \sqrt{\frac{c\ln n}{n}}\right)$ and $\lambda_{\min} = \tau\left(1 - \sqrt{\frac{c\ln n}{n}}\right)$, and the last equality (9) follows from the fact that $\frac{|\lambda|^2}{\sqrt{2|\lambda|^2-\tau^2}} = \left(\frac{2}{|\lambda|^2} - \frac{\tau^2}{|\lambda|^4}\right)^{-1/2}$ reaches its maximum either $|\lambda|$ is set to either upper bound $\lambda_{\max}$ or lower bound $\lambda_{\min}$. In the following, we prove that each term in the max bracket (9) is no more than $t = 1 + \frac{(2c+\varepsilon)\ln n}{n}$. For the former part $\frac{\lambda_{\max}^2}{\tau\sqrt{2\lambda_{\max}^2-\tau^2}} \le t$, this inequality is equivalent to

$$t \cdot \sqrt{1 - \sqrt{1 - t^{-2}}} \le \frac{\lambda_{\max}}{\tau} \le t \cdot \sqrt{1 + \sqrt{1 - t^{-2}}}. \tag{10}$$

The lower bound in (10) is obvious and for the upper bound, we have

$$t \cdot \sqrt{1 + \sqrt{1 - t^{-2}}} = 1 + \sqrt{\frac{(c+\varepsilon/2)\ln n}{n}} + o\left(\sqrt{\frac{\ln n}{n}}\right) \ge 1 + \sqrt{\frac{c\ln n}{n}} = \frac{\lambda_{\max}}{\tau}.$$

For the latter part $\frac{\lambda_{\min}^2}{\tau\sqrt{2\lambda_{\min}^2-\tau^2}} \le t$, this inequality is equivalent to

$$t \cdot \sqrt{1 - \sqrt{1 - t^{-2}}} \le \frac{\lambda_{\min}}{\tau} \le t \cdot \sqrt{1 + \sqrt{1 - t^{-2}}}. \tag{11}$$

The upper bound of (11) is obvious, and for the lower bound, we have

$$t \cdot \sqrt{1 - \sqrt{1 - t^{-2}}} = 1 - \sqrt{\frac{(c+\varepsilon/2)\ln n}{n}} + o\left(\sqrt{\frac{\ln n}{n}}\right) \le 1 - \sqrt{\frac{c\ln n}{n}} = \frac{\lambda_{\min}}{\tau}.$$

Therefore, we can obtain $(1 + (2c+\varepsilon)\cdot\frac{\ln n}{n})^n$ as an upper bound for our $\mathsf{RD}_2(D_\beta^n \| D_{\alpha\mathbf{S}})$. At last, applying the inequality $\left(1 + \frac{1}{x}\right)^x < e$ for all $x > 0$ completes the proof of theorem 6.11. □

Instantiation. As Theorem 6.3 stated, the distributions $\mathcal{S}, \mathcal{S}_1, \mathcal{S}_2$ can be set as $U_{B_1,B_2}(\mathbf{B}), D_{R,\sigma'}^{\mathsf{Coeff}(\mathbf{B})}, D_{R,\sigma}^{\mathsf{Coeff}(\mathbf{B})}$ respectively. By Lemma 2.13 in Section 2.6.4, $r \leftarrow D_{R,\sigma'}^{\mathsf{Coeff}(\mathbf{B})}$ should be invertible with non-negligible probability, and

$$\mathsf{RD}\left(\mathsf{Coeff}_{\mathbf{B}}\left(D_{R,\sigma}^{\mathsf{Coeff}(\mathbf{B})}\right) \| \mathsf{Rot}_{\mathbf{B}}(s) \cdot \mathsf{Coeff}_{\mathbf{B}}\left(D_{R,\sigma'}^{\mathsf{Coeff}(\mathbf{B})}\right)\right) \le \mathsf{poly}(\lambda).$$

According to Theorem 6.11, we can set $\sigma' = O(\sqrt{n \log n} \cdot p^{\frac{1}{g}}), \sigma = \tau\sigma' = O(\tau\sqrt{n \log n} \cdot p^{\frac{1}{g}}), B_1 = \frac{\tau}{n}\sqrt{\frac{c \ln n}{n}}, B_2 = \tau$, where $\tau = \mathsf{poly}(n)$ is a flexible polynomial that we will determine later.

Lemma 6.15 ((A)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}'}$ to $\mathsf{ent\text{-}dRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$)**.** *For any oracle solving the* $\mathsf{ent\text{-}dRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$ *problem with advantage ε, there exists an $i \in \{1, \cdots, g\}$ and an efficient algorithm that solves (A)-D-$\mathsf{RLWR}^i_{q,p,\mathbf{B},\ell,\mathcal{S}'}$ with advantage ε/g using this oracle.*

Sketch. This lemma can be proved by a simple hybrid argument. As the hybrid argument is standard, we just sketch the main idea: suppose there exists an algorithm that solves $\mathsf{ent\text{-}dRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}'}$ with advantage ε, i.e., it distinguishes $L_{s,q,p}(R, \mathbf{B})$ from uniformly random samples. Then the algorithm must be able to distinguish some neighboring hybrids, i.e., $L^i_{s,q,p}(R, \mathbf{B})$ and $L^{i-1}_{s,q,p}(R, \mathbf{B})$, with advantage ε/g, as there are g intermediate hybrids. □

The proof of Theorem 6.3 follows from Lemmas 6.5, 6.8, 6.10, and 6.15.

Remark 6.16. *We note that the reduction in Theorem 6.3 is not sample preserving, as the number of samples depends on the advantage of the decision* RLWR *distinguisher. However, as our target is to establish the pseudorandomness of a special entropic* RLWR *problem (with Gaussian distribution of secrets) with poly-modulus, we can only derive a reduction from search entropic* RLWE *to* $\frac{1}{\mathsf{poly}(\lambda)}$*-secure decision entropic* RLWR *due to that the reduction in Theorem 6.1 only holds for a bounded number of samples. Nevertheless, we can apply the hardness amplification technique of [Tes11] to achieve* $\mathsf{negl}(\lambda)$*-security by a parallel repetition up to $\omega(1)$ times.*

Remark 6.17. *To further establish the pseudorandomness of* RLWR *with Gaussian distribution of secrets from standard assumptions, two points are worth to mention. On one hand, the distribution $\mathcal{S}$ of* $\mathsf{ent\text{-}sRLWR}_{q,p,\mathbf{B},\ell,\mathcal{S}}$ *should satisfy that $\mathcal{S} \subseteq R_q^*$ by Theorem 6.1. This can be achieved by Theorem 6.11 and the instantiation of $\mathcal{S}$ (e.g., $U_{B_1,B_2}(\mathbf{B})$ with certain parameters B_1 and B_2). On the other hand, $\mathcal{S}$ should have enough entropy to guarantee the hardness of entropic* RLWE *with secret distribution $\mathcal{S}$ by Corollary 6.2. To be more concrete, $\mathcal{S}$ should satisfy that $\nu_\sigma(\mathcal{S}) \geq H_\infty(\mathcal{S}) - \sqrt{2\pi n}\log(e) \cdot \frac{r}{\sigma} \geq n\log(\gamma \cdot \sqrt{n}\log(n)) + \omega(\log(\lambda))$, where $r \leq 2\tau$ is the ℓ_2 upper bound of $\mathcal{S}$. To this end, we can set $\tau = O(\gamma \cdot n^2\sqrt{\log n}), \sigma = n\tau = O(\gamma \cdot n^3\sqrt{\log n})$.*

Acknowledgement. We thank the anonymous reviewers for their careful examination of our work and their constructive suggestions. Haoxiang Jin is supported by NSF CNS-2247727 and NRF award NRF-NRFI09-0005. Feng-Hao Liu is supported by NSF CNS-2402031. Zhedong Wang is supported by Young Elite Scientists Sponsorship Program by China Association for Science and Technology (YESS20220150), National Cryptologic Science Fund of China (No.2025NCSF02036). Yang Yu is supported by the National Natural Science Foundation of China (12441104) and the National Key R&D Program of China (2023YFA1009500).

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 595–618. Springer, Berlin, Heidelberg, August 2009. 2, 7, 8, 16, 17, 26, 29

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *USENIX Security 2016*, pages 327–343. USENIX Association, August 2016. 5

[AKPW13] Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs. Learning with rounding, revisited - new reduction, properties and applications. In Canetti and Garay [CG13], pages 57–74. 1, 2, 3, 4, 5, 6, 11, 19, 22, 25, 26, 32, 33, 55, 59, 71

[Bar89] David A. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in nc1. *Journal of Computer and System Sciences*, 38(1):150–164, 1989. 50, 51

[BBF+19] Hayo Baan, Sauvik Bhattacharya, Scott Fluhrer, Oscar Garcia-Morchon, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. Round5: Compact and fast post-quantum public-key encryption. Cryptology ePrint Archive, Paper 2019/090, 2019. `https://eprint.iacr.org/2019/090`. 2, 4

[BBPS19] Madalina Bolboceanu, Zvika Brakerski, Renen Perlman, and Devika Sharma. Order-LWE and the hardness of ring-LWE with entropic secrets. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 91–120. Springer, Cham, December 2019. 15

[BD20a] Zvika Brakerski and Nico Döttling. Hardness of LWE on general entropic distributions. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 551–575. Springer, Cham, May 2020. 2, 6, 8, 18, 22, 26, 30, 62, 66

[BD20b] Zvika Brakerski and Nico Döttling. Lossiness and entropic hardness for ring-LWE. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 1–27. Springer, Cham, November 2020. 2, 5, 17, 18

[BGG+14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer, Berlin, Heidelberg, May 2014. 50, 51

[BGM+16] Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen. On the hardness of learning with rounding over small modulus. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 209–224. Springer, Berlin, Heidelberg, January 2016. 8

[BJRW22] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. Entropic hardness of module-LWE from module-NTRU. In Takanori Isobe and Santanu Sarkar, editors, *INDOCRYPT 2022*, volume 13774 of *LNCS*, pages 78–99. Springer, Cham, December 2022. 2

[BJRW23] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. On the hardness of module learning with errors with short distributions. *Journal of Cryptology*, 36(1):1, January 2023. 30

[BKPW12] Mihir Bellare, Eike Kiltz, Chris Peikert, and Brent Waters. Identity-based (lossy) trapdoor functions and applications. In Pointcheval and Johansson [PJ12], pages 228–245. 2, 3

[BL17] Xavier Boyen and Qinyi Li. All-but-many lossy trapdoor functions from lattices and applications. In Katz and Shacham [KS17], pages 298–331. 2, 50, 52

[BLL+15] Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 3–24. Springer, Berlin, Heidelberg, November / December 2015. 10, 11

[BLMR13] Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan. Key homomorphic PRFs and their applications. In Canetti and Garay [CG13], pages 410–428. 3

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013. 1, 7, 8, 16, 29

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In Pointcheval and Johansson [PJ12], pages 719–737. 1, 2, 10, 16

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In Moni Naor, editor, *ITCS 2014*, pages 1–12. ACM, January 2014. 50, 51

[CG13] Ran Canetti and Juan A. Garay, editors. *CRYPTO 2013, Part I*, volume 8042 of *LNCS*. Springer, Berlin, Heidelberg, August 2013. 44, 45, 46

[Cona] Keith Conrad. The different ideal. Expository papers. Available at: `https://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf`. 13

[Conb] Keith Conrad. Factoring ideals after dedekind. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf`. 14

[DGI+19] Nico Döttling, Sanjam Garg, Yuval Ishai, Giulio Malavolta, Tamer Mour, and Rafail Ostrovsky. Trapdoor hash functions and their applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 3–32. Springer, Cham, August 2019. 2, 3

[DKRV18] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT 18*, volume 10831 of *LNCS*, pages 282–305. Springer, Cham, May 2018. 2, 4

[GAL13] M. Gil, F. Alajaji, and T. Linder. Rényi divergence measures for commonly used univariate continuous distributions. *Information Sciences*, 249:124–131, 2013. 40

[Ger31] S. Gerschgorin. Uber die abgrenzung der eigenwerte einer matrix. *Izvestija Akademii Nauk SSSR, Serija Matematika*, 7(3):749–754, 1931. 41

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In Andrew Chi-Chih Yao, editor, *ICS 2010*, pages 230–240. Tsinghua University Press, January 2010. 2

[GMP19] Nicholas Genise, Daniele Micciancio, and Yuriy Polyakov. Building an efficient lattice gadget toolkit: Subgaussian sampling and more. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 655–684. Springer, Cham, May 2019. 31, 32

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Canetti and Garay [CG13], pages 75–92. 51, 52

[HHK+24] Dennis Hofheinz, Kristina Hostáková, Julia Kastner, Karen Klein, and Akin Ünal. Compact selective opening security from LWE. In Qiang Tang and Vanessa Teague, editors, *PKC 2024, Part II*, volume 14604 of *LNCS*, pages 127–160. Springer, Cham, April 2024. 3, 4, 50, 52, 62

[Hof12] Dennis Hofheinz. All-but-many lossy trapdoor functions. In Pointcheval and Johansson [PJ12], pages 209–227. 34, 49, 60, 61, 62

[KR19] Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. Cryptology ePrint Archive, Paper 2019/302, 2019. `https://eprint.iacr.org/2019/302`. 2

[KS17] Jonathan Katz and Hovav Shacham, editors. *CRYPTO 2017, Part III*, volume 10403 of *LNCS*. Springer, Cham, August 2017. 45, 46

[LLW20] Qiqi Lai, Feng-Hao Liu, and Zhedong Wang. Almost tight security in lattices with polynomial moduli - PRF, IBE, all-but-many LTF, and more. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 652–681. Springer, Cham, May 2020. 52

[LLZ+18] Xianhui Lu, Yamin Liu, Zhenfei Zhang, Dingding Jia, Haiyang Xue, Jingnan He, Bao Li, and Kunpeng Wang. LAC: Practical ring-LWE based public-key encryption with byte-level modulus. Cryptology ePrint Archive, Report 2018/1009, 2018. 5

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Berlin, Heidelberg, May / June 2010. 13, 16, 38

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 35–54. Springer, Berlin, Heidelberg, May 2013. 2, 67

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *DCC*, 75(3):565–599, 2015. 16

[LSSS17] Benoît Libert, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. All-but-many lossy trapdoor functions and selective opening chosen-ciphertext security from LWE. In Katz and Shacham [KS17], pages 332–364. 2, 34, 50, 52, 56, 57

[LTV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In Howard J. Karloff and Toniann Pitassi, editors, *44th ACM STOC*, pages 1219–1234. ACM Press, May 2012. 18

[LW20] Feng-Hao Liu and Zhedong Wang. Rounding in the rings. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 296–326. Springer, Cham, August 2020. 2, 5, 8, 10, 19, 34, 37, 66, 68

[LWZW24] Hao Lin, Mingqiang Wang, Jincheng Zhuang, and Yang Wang. Hardness of entropic module-lwe. *Theor. Comput. Sci.*, 999(C), July 2024. 2

[MM11] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 465–484. Springer, Berlin, Heidelberg, August 2011. 1, 7, 19, 29, 30

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In Pointcheval and Johansson [PJ12], pages 700–718. 1, 6, 7, 30, 31

[MS23] Daniele Micciancio and Adam Suhl. Simulation-secure threshold PKE from LWE with polynomial modulus. Cryptology ePrint Archive, Report 2023/1728, 2023. 7, 8, 29, 30, 31

[NR23] Parker Newton and Silas Richelson. A lower bound for proving hardness of learning with rounding with polynomial modulus. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 805–835. Springer, Cham, August 2023. 2, 5

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 333–342. ACM Press, May / June 2009. 1, 16

[Pei10] Chris Peikert. An efficient and parallel Gaussian sampler for lattices. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Berlin, Heidelberg, August 2010. 18

[Pei16a] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016. 1

[Pei16b] Chris Peikert. How (not) to instantiate ring-LWE. In Vassilis Zikas and Roberto De Prisco, editors, *SCN 16*, volume 9841 of *LNCS*, pages 411–430. Springer, Cham, August / September 2016. 15, 16, 17

[PJ12] David Pointcheval and Thomas Johansson, editors. *EUROCRYPT 2012*, volume 7237 of *LNCS*. Springer, Berlin, Heidelberg, April 2012. 45, 46, 47

[PP19] Chris Peikert and Zachary Pepin. Algebraically structured LWE, revisited. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 1–23. Springer, Cham, December 2019. 16, 17

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *49th ACM STOC*, pages 461–473. ACM Press, June 2017. 17

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 187–196. ACM Press, May 2008. 2, 3, 19

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005. 1, 16

[Rén61] Alfréd Rényi. On measures of entropy and information. Proc. 4th Berkeley Symp. Math. Stat. Probab. 1, 547-561, 1961. 10

[Rib89] Paulo Ribenboim. *How are the Prime Numbers Distributed?*, pages 153–254. Springer US, New York, NY, 1989. 7, 29

[RS62] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6(1):64 – 94, 1962. 28

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994. 1

[SS13] Damien Stehlé and Ron Steinfeld. Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004, 2013. 15

[Ste04] William Stein. A brief introduction to classical and adelic algebraic number theory, 2004. `https://wstein.org/129/ant/ant.pdf`, last accessed 16 Otc 2024. 13

[Tes11] Stefano Tessaro. Security amplification for the cascade of arbitrarily weak PRPs: Tight bounds via the interactive hardcore lemma. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 37–54. Springer, Berlin, Heidelberg, March 2011. 5, 43

Supplementary Material

A All-but-many Lossy Trapdoor Functions (ABM-LTF)

Next we give the definition of all-but-many lossy trapdoor functions (ABM-LTF) [Hof12].

Definition A.1 ([Hof12])**.** *An all-but-many lossy trapdoor function (ABM-LTF) scheme* ABM *with domain* $\mathcal{S}$ *and range* $\mathcal{Y}$ *includes the following algorithms:*

- ***Key Generation.*** $\mathsf{ABM.Gen}(1^\lambda)$ *generates an evaluation key* ek*, an inversion key* ik *and a tag key* tk*. The evaluation key* ek *specifies a tag set* $\mathcal{T} = \mathcal{T}_c \times \mathcal{T}_a$ *that contains two disjoint sets of injective tags* $\mathcal{T}_{\mathsf{inj}}$ *and lossy tags* $\mathcal{T}_{loss}$*. Every tag* $t = (t_\mathsf{c}, t_\mathsf{a})$ *is composed of a core part* $t_\mathsf{c} \in \mathcal{T}_\mathsf{c}$ *and an auxiliary part* $t_\mathsf{a} \in \mathcal{T}_\mathsf{a}$*.*
- ***Evaluation.*** $\mathsf{ABM.Eval}(\mathsf{ek}, t, \boldsymbol{s})$ *inputs an evaluation key, a tag* $t \in \mathcal{T}$ *and a preimage* $\boldsymbol{s} \in \mathcal{S}$*, and outputs the image* $\boldsymbol{y} = f_{\mathsf{ek},t}(\boldsymbol{s})$*.*
- ***Inversion.*** $\mathsf{ABM.Invert}(\mathsf{ik}, y)$ *inputs an inversion key* ik*, a tag* $t \in \mathcal{T}$ *and* $y \in \mathcal{Y}$*, and outputs the unique preimage* $\boldsymbol{s} = f^{-1}_{\mathsf{ik},t}(\boldsymbol{y})$ *such that* $\boldsymbol{y} = f_{\mathsf{ek},t}(\boldsymbol{s})$*.*
- ***Lossy Tag Labeling.*** $\mathsf{ABM.LTag}(\mathsf{tk}, t_\mathsf{a})$ *inputs a tag key* tk *and auxiliary part of a tag* $t_\mathsf{a} \in \mathcal{T}_{\mathsf{aux}}$*, and outputs a core part* $t_\mathsf{c} \in \mathcal{T}_{\mathsf{core}}$ *such that* $(t_\mathsf{c}, t_\mathsf{a}) \in \mathcal{T}_{\mathsf{loss}}$*.*
- ***Lossy Tag Judgement.*** $\mathsf{ABM.isLossy}(\mathsf{tk}, t)$ *judges whether the tag* $t \in \mathcal{T}$ *is a lossy tag. If* $t \in \mathcal{T}_{\mathsf{loss}}$*, return 1; Otherwise, return 0.*

We consider the following properties of ABM-LTF*:*

- ***Correctness.*** *For key pair* $(\mathsf{ek}, \mathsf{ik}) \leftarrow \mathsf{ABM.Gen}(1^\lambda)$*, we require that for all* $\boldsymbol{s} \in \mathcal{S}$*, with overwhelming probability over* $\mathsf{ABM.Gen}(1^\lambda)$ *that* $x = f^{-1}_{\mathsf{ik}}(f_{\mathsf{ek}}(x))$*.*
- ***Expansion.*** *We define the expansion of* ABM-LTF *as* $\chi := \log|\mathcal{Y}|/\log|\mathcal{S}|$ *and we expect it to be a constant.*
- ***l-Lossiness.*** *We define that a* ABM-LTF *with l-lossiness (abbreviated by l-*ABM-LTF*) satisfies that for mutually correlated random variables* $(\boldsymbol{s}, \mathsf{aux})$*,* $(\mathsf{ek}, \mathsf{ik}, \mathsf{tk}) \leftarrow \mathsf{ABM.Gen}(1^\lambda)$*, any* $t_\mathsf{a} \in \mathcal{T}_{\mathsf{aux}}$ *and* $t_\mathsf{c} \leftarrow \mathsf{ABM.LTag}(\mathsf{tk}, t_\mathsf{a})$*, we have*

$$H^{\mathsf{smooth}}_\infty(\boldsymbol{s} \mid \mathsf{ek}, t, f_{\mathsf{ek},t}(\boldsymbol{s}), \mathsf{aux}) \geq H^{\mathsf{smooth}}_\infty(\boldsymbol{s} \mid \mathsf{aux}) - l(\lambda)$$

- ***Indistinguishability.*** *Multiple lossy tags are computationally indistinguishable from random tags, i.e. for all* PPT *adversary* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{ABM},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}(1^\lambda, \mathsf{ek})^{\mathsf{ABM.LTag}(\mathsf{tk},\cdot)} = 1\right] - \Pr\left[\mathcal{A}(1^\lambda, \mathsf{ek})^{O_{\mathcal{T}_\mathsf{c}}(\cdot)} = 1\right]\right|$$

is negligible, where $(\mathsf{ek}, \mathsf{ik}, \mathsf{tk}) \leftarrow \mathsf{ABM.Gen}(1^\lambda)$ *and* $O_{\mathcal{T}_\mathsf{c}}(\cdot)$ *is an oracle that returns a uniform random core tag* $t_\mathsf{c} \leftarrow U(\mathcal{T}_\mathsf{c})$*.*

- ***Evasiveness.*** *We require that lossy tags are computationally hard to find with access to oracles outputting and judging lossy tags, i.e. for all* PPT *adversary* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathsf{EVA}}_{\mathsf{ABM},\mathcal{A}}(\lambda) := \Pr\left[\mathcal{A}(1^\lambda, \mathsf{ek})^{\mathsf{ABM.LTag}(\mathsf{tk},\cdot),\mathsf{ABM.isLossy}(\mathsf{tk},\cdot)} \in \mathcal{T}_{\mathsf{loss}}\right]$$

is negligible, where $(\mathsf{ek},\mathsf{ik},\mathsf{tk}) \leftarrow \mathsf{ABM.Gen}(1^\lambda)$ *and* $\mathcal{A}$ *never outputs a tag* $t = (t_{\mathsf{c}}, t_{\mathsf{a}})$ *such that* t_c *was queried from* ABM.LTag *oracle on* t_{a}*.*

We apply the similar strategy in [BL17, LSSS17, HHK+24] to build our ABM-LTF scheme based on our LTF construction, which is homomorphically evaluating a PRF circuit. We need the following lemma for homomorphic computation based on the gadget matrix $\mathbf{G}$ with general gadget base b.

Lemma A.2 (Homomorphic Computation [BGG+14, BV14])**.** *Let* λ *be a security parameter, and* $n, m, q = \mathsf{poly}(\lambda)$ *be lattice parameters. Let* $b > 0$ *be a gadget base such that* $k = \lceil \log_b q \rceil$ *is a constant and* $\mathbf{G} \in \mathbb{Z}_q^{kn\times n}$ *be the gadget matrix. Let* $m = kn$*. Let* $\{F_\lambda\}_{\lambda\in\mathbb{N}}$ *be a circuit family* $f : \{0,1\}^{u(\lambda)} \to \{0,1\}$ *with depth* $d = d(\lambda)$*. There exists a pair of efficient and deterministic algorithms* $(\mathsf{pubEval}, \mathsf{ctEval})$ *satisfying the following properties:*

- $\mathsf{pubEval}(f \in \mathcal{F}, \{\mathbf{B}_i \in \mathbb{Z}_q^{m\times n}\}_{i\in[u]}) \to \mathbf{B}_{\mathbf{x}} \in \mathbb{Z}_q^{m\times n}$;
- $\mathsf{ctEval}(f \in \mathcal{F}, \mathbf{A} \in \mathbb{Z}_q^{m\times n}, \{\mathbf{R}_i \in \mathbb{Z}_q^{m\times m}\}_{i\in[u]}, \mathbf{x} \in \{0,1\}^u) \to \mathbf{R}_{\mathbf{x}} \in \mathbb{Z}_q^{m\times m}$.

Furthermore, for all matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$*,* $\{\mathbf{R}_i \in \mathbb{Z}_q^{m\times m}\}_{i\in[u]}$*, input* $\mathbf{x} \in \{0,1\}^u$ *such that* $\mathbf{B}_i = \mathbf{R}_i \cdot \mathbf{A} + \mathbf{x}[i] \cdot \mathbf{G}$ *and* d*-depth Boolean circuit* $f \in \mathcal{F}$*, we have*

$$\mathbf{B}_{\mathbf{x}} = \mathbf{R}_{\mathbf{x}} \cdot \mathbf{A} + f(\mathbf{x}) \cdot \mathbf{G}$$

Let χ *be a* β*-bounded distribution over* $\mathbb{Z}_q$*. If for all* $\mathbf{R}_i \leftarrow \chi^{m\times m}$*, then*

$$\|\mathbf{R}_{\mathbf{x}}\|_\infty \le 2 \cdot 4^d \beta m^2 (b-1).$$

The proof of this lemma is similar to [BV14], while generalizing the base b from 2 to any positive integer $b < q$. We first need the result of Barrington's theorem from [Bar89].

Width-5 Permutation Branching Programs. We say that Π is a permutation branching program of length L with input space $\{0,1\}^\ell$ is a sequence of L tuples with the form $(\mathsf{var}(t), \sigma_{t,0}, \sigma_{t,1})$ if

- Function $\mathsf{var} : [L] \to [\ell]$ takes input as $t \in [L]$ and outputs $\mathsf{var}(t) \in [\ell]$, which associates t-th tuple with bit $x_{\mathsf{var}(t)}$.
- For all $t \in [L]$ and $i \in 0, 1$, $\sigma_{t,i} \in S_5$ is a permutation on [5].

We next describe the computation procedure of the program Π on ℓ-bit input $\mathbf{x} = (x_1, \cdots, x_\ell)$. In each step $t \in [L]$, the program has a state $\zeta_t \in [5]$. Initially, program Π begins with starting state $\zeta_0 = 1$, computes each state recursively as $\zeta_t = \sigma_{t,\mathsf{var}(t)}(\zeta_{t-1})$ and obtains a final state ζ_L after L steps. The program Π outputs 1 if $\zeta_L = 1$, and 0 if $\zeta_L \in \{2,3,4,5\}$.

An important theoretical result in the relationship between a Boolean circuit C with two-input NAND gates and a width-5 permutation branching program is stated as below:

Theorem A.3 (Barrington's Theorem [Bar89])**.** *Every boolean circuit Ψ in two-input NAND gates with input $\{0,1\}^\ell$ and depth d can be transformed to a width-5 permutation branching program Π with length 4^d and same input and output as Ψ. Furthermore, the branching program Π can be computed in $\mathsf{poly}(\ell, 4^d)$ time with the description of Boolean NAND circuit Ψ.*

With these powerful tools, we next prove lemma A.2.

Proof of A.2. For every Boolean NAND circuit f with input $\mathbf{x} \in \{0,1\}^\ell$ and depth d, we apply the Barrington's theorem A.3 to f and obtain an equivalent width-5 permutation branching program Π with length $L = 4^d$. Thus, homomorphically evaluating the boolean circuit f is equivaleng to homomorphically evaluate the branching program Π.

For a GSW encoding $\mathbf{B} = \mathbf{R} \cdot \mathbf{A} + x\mathbf{G} \in \mathbb{Z}_q^{m\times n}$ such that $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, $\mathbf{R} \in \mathbb{Z}_q^{m\times m}$ and $x \in \{0,1\}$, we define $\mathbf{R}(\mathbf{B}) = \mathbf{R} \in \mathbb{Z}_q^{m\times m}$. We first describe the homomorphic evaluation procedure related to addition and multiplication of two GSW encodings $\mathbf{B}_i = \mathbf{R}_i \cdot \mathbf{A} + x_i\mathbf{G}$ for $i \in \{1,2\}$ [GSW13, BGG+14].

- For addition, $\mathsf{HomoAdd}(\mathbf{B}_1, \mathbf{B}_2) = \mathbf{B}_1 + \mathbf{B}_2$. It is obvious that $\mathbf{R}(\mathbf{B}_1 + \mathbf{B}_2) = \mathbf{R}_1 + \mathbf{R}_2$, indicating the norm bound $\|\mathbf{R}(\mathbf{B}_1 + \mathbf{B}_2)\|_\infty \le \|\mathbf{R}_1\|_\infty + \|\mathbf{R}_2\|_\infty$.
- For multiplication, $\mathsf{HomoMult}(\mathbf{B}_1, \mathbf{B}_2) = \mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{B_2}$. Rewrite the result with $\mathbf{A}$, $\mathbf{R}_i$ and x_i where $i \in \{1,2\}$, we have

$$\begin{aligned}\mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{B_2} &= \mathbf{G}^{-1}(\mathbf{B}_1) \cdot (\mathbf{R}_2 \cdot \mathbf{A} + x_2\mathbf{G}) \\ &= \mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{R}_2 \cdot \mathbf{A} + x_2\mathbf{B}_1 \\ &= (\mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{R}_2 + x_2\mathbf{R}_1) \cdot \mathbf{A} + x_1x_2\mathbf{G}.\end{aligned}$$

  Thus, we have $\mathbf{R}(\mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{B_2}) = \mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{R}_2 + x_2\mathbf{R}_1$ which is assymetric between two GSW encodings. Since every entry of $\mathbf{G}^{-1}(\mathbf{B}_1)$ is bounded by $b-1$, we have $\|\mathbf{R}(\mathbf{G}^{-1}(\mathbf{B}_1) \cdot \mathbf{B_2})\|_\infty \le m(b-1)\|\mathbf{R}_2\|_\infty + x_2\|\mathbf{R}_1\|_\infty$.

Same as [BV14], we represent each state $\zeta_t \in [5]$ by a binary vector $\mathbf{v}_t$ which is unit vector $\mathbf{u}_{\zeta_t}$ in 5 dimensions. It holds that for $t = 1, \cdots, L$ and $i \in [5]$,

$$\begin{aligned}\mathbf{v}_t[i] &= \mathbf{v}_{t-1}\left[\sigma_{t,0}^{-1}(i)\right] \cdot (1 - x_{\mathsf{var}(t)}) + \mathbf{v}_{t-1}\left[\sigma_{t,1}^{-1}(i)\right] \cdot x_{\mathsf{var}(t)} \\ &= \mathbf{v}_{t-1}[\gamma_{t,i,0}] \cdot (1 - x_{\mathsf{var}(t)}) + \mathbf{v}_{t-1}[\gamma_{t,i,1}] \cdot x_{\mathsf{var}(t)}\end{aligned}$$

where $\gamma_{t,i,0} = \sigma_{t,0}^{-1}(i)$ and $\gamma_{t,i,1} = \sigma_{t,1}^{-1}(i)$ can be publicly derived from the description of Π.

Homomorphic Evaluation of $\mathsf{pubEval}(\Psi, \mathbf{B}_1, \cdots, \mathbf{B}_u)$. The homomorphic evaluation procedure takes input as $\mathbf{B}_i = \mathbf{R}_i \cdot \mathbf{A} + x_i\mathbf{G}$ for $i \in [u]$ and $\mathbf{R}_i \leftarrow \chi^{m\times m}$. Since χ is a β-bounded distribution, it is easy to verify that $\|\mathbf{R}_i\|_\infty \le m\beta$.

We maintain a GSW encoding vector $\mathbf{V}_t = (\mathbf{V}_{t,1}, \mathbf{V}_{t,2}, \mathbf{V}_{t,3}, \mathbf{V}_{t,4}, \mathbf{V}_{t,5})$ related to state vector $\mathbf{v}_t[i]$ for each $t \in \{0, 1, \cdots, L\}$, i.e $\mathbf{V}_{t,i} \in \mathbb{Z}_q^{m\times n}$ is a GSW encoding of $\mathbf{v}_t[i]$ for each $t \in \{0, 1, \cdots, L\}$ and $i \in [5]$ and we denote $\mathbf{R}_{t,i} = \mathbf{R}(\mathbf{V}_{t,j})$.

- **Initialization.** Initialize the 0 state as $\mathbf{V}_{0,i} := \mathbf{v}_0[i] \cdot \mathbf{G}$. Note that $\mathbf{V}_{0,i}$ is a valid GSW encoding for $\mathbf{v}_0[i]$ with $\mathbf{R}_{0,i} = \mathbf{0}$.

  Compute the GSW encodings of the complements of input bits as $\bar{\mathbf{B}}_j = \mathbf{G} - \mathbf{B}_j$. It is obvious that $\bar{\mathbf{B}}_j$ is a valid GSW encoding of $1 - x_j$ with $\bar{\mathbf{R}}_j := \mathbf{R}(\bar{\mathbf{B}}_j) = -\mathbf{R}_i$ for every $j \in [u]$.

- **Evaluation.** The evaluation procedure proceeds iteratively for $t \in [L]$. Given $\mathbf{V}_{t-1} = (\mathbf{V}_{t-1,1}, \mathbf{V}_{t-1,2}, \mathbf{V}_{t-1,3}, \mathbf{V}_{t-1,4}, \mathbf{V}_{t-1,5})$, we compute $\mathbf{V}_t$ by

$$\mathbf{V}_{t,i} = \mathsf{HomoAdd}\left(\mathsf{HomoMult}\left(\mathbf{V}_{t-1,\gamma_{t,i,0}}, \bar{\mathbf{B}}_{\mathsf{var}(t)}\right), \mathsf{HomoMult}\left(\mathbf{V}_{t-1,\gamma_{t,i,1}}, \mathbf{B}_{\mathsf{var}(t)}\right)\right)$$

  for $i \in [5]$.

- **Output.** Output $\mathbf{V}_{L,1}$.

The procedure of $\mathsf{ctEval}(\Psi, \mathbf{A}, \{\mathbf{R}_i\}_{i\in[u]}, \mathbf{x})$ and the correctness is obvious so we omit it. We next use the induction on $t \in \{0, 1, \cdots, L\}$ to prove that $\|\mathbf{R}_{t,i}\|_\infty \le 2t\beta m^2(b-1)$.

This statement is no doubt true for $t = 0$. We assume that the statement holds for $t-1$, from the noise growth property of homomorphic evaluation, for $i \in [5]$, we have

$$\begin{aligned}\|\mathbf{R}_{t,i}\|_\infty &\le 2m(b-1)\|\mathbf{R}_{\mathsf{var}(t)}\|_\infty + \left(1 - x_{\mathsf{var}(t)}\right)\|\mathbf{R}_{t-1,\gamma_{t,i,0}}\|_\infty + x_{\mathsf{var}(t)}\|\mathbf{R}_{t-1,\gamma_{t,i,1}}\|_\infty \\ &\le 2m^2\beta(b-1) + 2(t-1)m^2\beta(b-1) \qquad (12) \\ &= 2tm^2\beta(b-1)\end{aligned}$$

where (12) follows the induction assumption, the upper bound for $\|\mathbf{R}_{\mathsf{var}(t)}\|_\infty$ and exactly one of $x_{\mathsf{var}(t)}$ and $1 - x_{\mathsf{var}(t)}$ is 1. Thus, the statement holds for t.

We choose the case $t = L \le 4^d$ and complete the proof. □

In [BL17, LSSS17, HHK+24], the authors utilized pseudorandom function PRF, where our lossy ABM-LTF tag (t_c, t_a) is defined by a PRF key $K \in \{0,1\}^k$ such that $t_c = \mathsf{PRF}_K(t_a)$. We encodes each bit of K, then the evaluation key ek consists of λ GSW encodings and both inversion key ik and tag key tk includes the PRF key K. In the evaluation (resp. inversion) step, we apply homomorphic evaluation in the public (resp. private) way from lemma A.2 to the PRF evaluation circuit.

However, there is no known construction for lattice-based PRF scheme in NC1 so that directly doing homomorphic computation to the PRF evaluation circuit results in a super-polynomial modulus q. In order to guarantee a polynomial modulus q, we need to apply the method in [LLW20], which is using a fully homomorphic encryption scheme HE, evaluating the PRF circuit by HE.Eval instead of pubEval to get a HE ciphertext HE.ct related to the PRF value, and then evaluate HE.Dec on the GSW encodings of HE.sk and HE.ct by pubEval to get a GSW encoding of the PRF value. The homomorphic encryption scheme is defined as follows.

Definition A.4 (Fully Homomorphic Encryption [GSW13])**.** HE *is a special kind of* PKE *with an additional public evaluation key* hevk *generated in* HE.Gen*, an additional evaluation* PPT *algorithm* HE.Eval *and message space* $\mathcal{M} = \{0,1\}$*:*

- $\mathsf{HE.Gen}(1^\lambda)$*: Input a security parameter* λ*, output a public key* hek*, a public evaluation key* hevk *and a secret decryption key* hdk*.*

- $\mathsf{HE.Eval}(\mathsf{hevk}, C, \mathsf{ct}_1, \cdots, \mathsf{ct}_l)$*: Input an evaluation key* evk*, homomorphically evaluate a circuit* $f : \{0,1\}^l \to \{0,1\}$ *on* $\mathsf{ct}_1, \cdots, \mathsf{ct}_l$*, and output a ciphertext* ct_f*.*

We require HE *scheme has full homomorphism and compactness.*

- ***Full homomorphism.*** *For any boolean circuit C with polynomial depth $L = L(\lambda)$, and any messages $\mathsf{msg}_1, \cdots, \mathsf{msg}_l \in \{0,1\}$, we have*

$$\Pr[\mathsf{HE.Dec}(\mathsf{hdk}, \mathsf{HE.Eval}(\mathsf{hevk}, C, \{\mathsf{ct}_i\}_{i\in[l]})) = f(\mathsf{msg}_1, \cdots, \mathsf{msg}_l)] = 1 - \mathsf{negl}(\lambda),$$

  where $(\mathsf{hek}, \mathsf{hevk}, \mathsf{hdk}) \leftarrow \mathsf{HE.Gen}(1^\lambda)$ *and* $\mathsf{ct}_i \leftarrow \mathsf{HE.Enc}(\mathsf{hek}, \mathsf{msg}_i)$.

- ***Compactness.*** *The decryption circuit is independent of the evaluated circuit C.*

With all the definitions above, we can construct our compact ABM scheme.

Construction A.5. *Let λ be a security parameter and $n, m, q = \mathsf{poly}(\lambda)$ be lattice parameters. Let $\mathcal{S}$ be our entropic preimage distribution over $\mathbb{Z}_q^n$ and $\mathcal{Y} = \mathbb{Z}_p^{2m}$ be the image set. Let $\mathsf{PRF} : \{0,1\}^{k_0} \times \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ be a secure pseudorandom function with key length $k_0 = k_0(\lambda)$, input length $k_1 = k_1(\lambda)$ and output length $k_2 = k_2(\lambda)$. Let $\mathsf{HE} = (\mathsf{HE.KeyGen}, \mathsf{HE.Enc}, \mathsf{HE.Dec}, \mathsf{HE.Eval})$ be a fully homomorphic encryption scheme with $g = g(\lambda)$ as the secret key length, $g' = g'(\lambda)$ as the ciphertext length and $d = d(\lambda)$ as the depth of decryption circuit* HE.Dec*. Let* $(\mathsf{pubEval}, \mathsf{ctEval})$ *be the homomorphic computation algorithms. Our* ABM-LTF *scheme includes the following algorithms:*

- $\mathsf{ABM.Gen}(1^\lambda)$:

  1. Sample a lossy matrix $\mathbf{A} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$ and a uniformly random PRF key $K \xleftarrow{\$} \{0,1\}^{k_0}$. Define the tag space as $\mathcal{T} = \{0,1\}^{k_2} \times \{0,1\}^{k_1}$, the core part of tag space as $\mathcal{T}_\mathsf{c} = \{0,1\}^{k_2}$ and the auxiliary part of tag space as $\mathcal{T}_\mathsf{a} = \{0,1\}^{k_1}$;
  2. Sample HE keys $(\mathsf{hek}, \mathsf{hevk}, \mathsf{hdk}) \leftarrow \mathsf{HE.KeyGen}(1^\lambda)$ and describe the decryption algorithm HE.Dec as a NAND Boolean circuit C_Dec;
  3. Encrypt each bit of K by HE: $d_i \xleftarrow{\$} \mathsf{HE.Enc}(\mathsf{hek}, K_i)$ for $i \in [k_0]$;
  4. Sample $\mathbf{R}_{\mathbf{D}_i} \xleftarrow{\$} \chi^{m\times m}$ and compute $\mathbf{D}_i = \mathbf{R}_{\mathbf{D}_i} \cdot \mathbf{A} + \mathsf{hdk}_i \cdot \mathbf{G}$ for each $i \in [g]$, where hdk_i denotes i-th bit of hdk;
  5. Sample $\mathbf{R}_\mathsf{ent} \xleftarrow{\$} [-b^2, b^2]^{m\times m} \in \mathbb{Z}_q^{m\times m}$ and compute $\mathbf{A}_\mathsf{ent} = \mathbf{R}_\mathsf{ent} \cdot \mathbf{A}$;
  6. Output the evaluation key $\mathsf{ek} = (\mathbf{A}, \mathbf{A}_\mathsf{ent}, \{d_i\}_{i\in[k_0]}, \{\mathbf{D}_i\}_{i\in[g]}, \mathsf{hek}, \mathsf{hevk})$, the inversion key $\mathsf{ik} = (\{\mathbf{R}_{\mathbf{D}_i}\}_{i\in[g]}, \mathbf{R}_\mathsf{ent}, \mathsf{hdk}, K)$ and the tag key $\mathsf{tk} = K$.

- $\mathsf{ABM.Eval}(\mathsf{ek}, t, \boldsymbol{s})$: Input $\mathsf{ek} = (\mathbf{A}, \mathbf{A}_\mathsf{ent}, \{d_i\}_{i\in[k_0]}, \{\mathbf{D}_i\}_{i\in[g]}, \mathsf{hek}, \mathsf{hevk})$, a preimage $\boldsymbol{s} \in \mathbb{Z}_q^n$ and a tag $t = (t_\mathsf{c}, t_\mathsf{a}) \in \{0,1\}^{k_2} \times \{0,1\}^{k_1}$.

  1. Let RC_t be a circuit which is hardwired the tag t and takes a pseudorandom key $K \in \{0,1\}^{k_0}$ as input, and judge the tag whether is lossy or not:

$$\mathsf{RC}_t := \begin{cases} 0, & \text{if } t_\mathsf{c} = \mathsf{PRF}_K(t_\mathsf{a}); \\ 1, & \text{otherwise.} \end{cases}$$

  2. Homomorphically evaluate the circuit RC_t on the HE ciphertexts of PRF key K by HE.Eval, i.e.

$$\mathsf{ct} = \mathsf{HE.Eval}(\mathsf{hevk}, \mathsf{RC}_t, \{d_i\}_{i\in[k_0]});$$

3. Homomorphically evaluate the decryption circuit C_{Dec} on the GSW encodings $\{\mathbf{D}_i\}_{i\in[g]}$ and $\{\mathsf{ct}_j\mathbf{G}\}_{j\in[g']}$ where ct_j denotes the j-th bit of ct, i.e.

$$\mathbf{A}_{\mathsf{pub}} \leftarrow \mathsf{pubEval}\left(C_{\mathsf{Dec}}, \{\mathbf{D}_i\}_{i\in[g]}, \{\mathsf{ct}_j\mathbf{G}\}_{j\in[g']}\right) \in \mathbb{Z}_q^{m\times n};$$

4. Add $\mathbf{A}_{\mathsf{ent}}$ to $\mathbf{A}_{\mathsf{pub}}$: $\mathbf{A}_1 \leftarrow \mathbf{A}_{\mathsf{pub}} + \mathbf{A}_{\mathsf{ent}}$;
5. Compute and output

$$\boldsymbol{y} \leftarrow \left\lfloor \begin{pmatrix}\mathbf{A}\\ \mathbf{A}_1\end{pmatrix} \cdot \boldsymbol{s} \right\rceil_p \in \mathbb{Z}_p^{2m}.$$

- $\mathsf{ABM.LTag}(\mathsf{tk}, t_{\mathsf{a}})$: Input tag key $\mathsf{tk} = K$ and an auxiliary tag component $t_{\mathsf{a}} \in \{0,1\}^l$. Compute the core tag component $t_{\mathsf{c}} = \mathsf{PRF}(K, t_{\mathsf{a}}) \in \{0,1\}^{k_2}$.
- $\mathsf{ABM.Invert}(\mathsf{ek}, \mathsf{ik}, t, \boldsymbol{y})$: Input $\mathsf{ek} = (\mathbf{A}, \mathbf{A}_{\mathsf{ent}}, \{d_i\}_{i\in[k_0]}, \{\mathbf{D}_i\}_{i\in[g]}, \mathsf{hek}, \mathsf{hevk})$, $\mathsf{ik} = (\{\mathbf{R}_{\mathbf{D}_i}\}_{i\in[g]}, \mathbf{R}_{\mathsf{ent}}, \mathsf{hdk}, K)$, an injective tag $t = (t_{\mathsf{c}}, t_{\mathsf{a}})$ and an image $\boldsymbol{y} \in \mathbb{Z}_p^{2m}$,
  1. Return $\perp$ if $t_{\mathsf{c}} = \mathsf{PRF}(K, \mathsf{a})$;
  2. Homomorphically evaluate the circuit RC_t on the HE ciphertexts of PRF key K by HE.Eval, i.e.

$$\mathsf{ct} = \mathsf{HE.Eval}(\mathsf{hevk}, \mathsf{RC}_t, \{d_i\}_{i\in[k_0]});$$

  3. Using ctEval to compute the Matrix

$$\mathbf{R}_{\mathsf{ct}} \leftarrow \mathsf{ctEval}\left(C_{\mathsf{Dec}}, \mathbf{A}, \{\mathsf{hdk}_i\}_{i\in[g]}, \{\mathsf{ct}_j\}_{j\in[g']}, \{\mathbf{R}_{\mathbf{D}_i}\}_{i\in[g]}, \{[0]_i\}_{i\in[g']}\right) \in \mathbb{Z}_q^{m\times m};$$

  4. Add $\mathbf{R}_{\mathsf{ent}}$ to $\mathbf{R}_{\mathsf{ct}}$ in order to provide enough entropy: $\mathbf{R} \leftarrow \mathbf{R}_{\mathsf{ct}} + \mathbf{R}_{\mathsf{ent}}$;
  5. Let $\bar{\mathbf{A}} \leftarrow \begin{pmatrix}\mathbf{A}\\ \mathbf{R}\cdot\mathbf{A}+\mathbf{G}\end{pmatrix} \in \mathbb{Z}_q^{2m\times n}$. Compute the gadget trapdoor $\mathbf{T}_{\bar{\mathbf{A}}} \leftarrow \begin{pmatrix}-\mathbf{R} & \mathbf{I}_m\end{pmatrix} \in \mathbb{Z}_q^{m\times 2m}$ of $\bar{\mathbf{A}}$;
  6. Run the LWR inversion algorithm to return the preimage

$$\boldsymbol{s} \leftarrow \mathsf{LWRInvert}(\mathbf{T}_{\bar{\mathbf{A}}}, \bar{\mathbf{A}}, \boldsymbol{y}) \in \mathbb{Z}_q^n.$$

Parameter Selection. Our goal is to achieve the five properties described in the A.1, we need the following restrictions:

- $\mathsf{LWE}_{\ell,m,q,\chi}$ is hard, $\beta^* = m\beta(b^2 + 2\cdot 4^d\beta m(b-1))$ and $q > p^* \geq nmp\beta^*$ to guarantee the pseudorandomness of lossy matrix and l-lossiness property of lossy mode;
- $k = \lceil \log_b q \rceil$ is a constant which is to ensure the constant expansion property of our ABM-LTF;
- $\mathsf{HNFLWE}_{n,n,q,\chi}$ is hard and $m = (k+2)n$ to achieve the pseudorandomness of our GSW encodings;
- $p \geq 2(b+1)(2\cdot 4^d\beta m^2(b-1) + mb^2 + 1)$ in order to make the LWR inversion algorithm recover the preimage successfully.
- $n \geq 2\ell$ and the least prime factor p_{min} of q satisfies $p_{\mathsf{min}} > b^2$. These are the prerequisite of applying leftover hash lemma.

Theorem A.6. *Let λ be the security parameter and guarantee the constraints of each parameter above. The consturction* $\mathsf{ABM} = (\mathsf{ABM.Gen}, \mathsf{ABM.LTag}, \mathsf{ABM.Eval}, \mathsf{ABM.Invert})$ *is an l-lossy* ABM *scheme which satisfies constant expansion, invertible correctness, indistinguishability and evasiveness.*

Lemma A.7 (Constant Expansion)**.** *Let $k = \lceil \log_b q \rceil$ be a constant and $m = kn$. If $\mathcal{S}$ covers $U(\mathbb{Z}_q^n)$, our LTF construction has $O(1)$ expansion.*

Proof. Given the public matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, for any tag t we compute the matrix $\mathbf{A}_1 \in \mathbb{Z}_q^{m \times n}$ as described in the function evaluation algorithm. For all $\mathbf{s} \in \mathbb{Z}_q^n$, we obtain the image $\boldsymbol{y} = \left\lfloor \begin{pmatrix} \mathbf{A} \\ \mathbf{A}_1 \end{pmatrix} \cdot \mathbf{s} \right\rceil_p \in \mathbb{Z}_p^{2m}$. Therefore, we compute the expansion as

$$\eta = \frac{2m \cdot \log p}{n \cdot \log q} = O(1).$$

□

Lemma A.8 (Correctness)**.** *Let $p \geq 2(b+1)(2 \cdot 4^d \beta m^2 (b-1) + mb^2 + 1)$. If* HE *is a fully homomorphic encryption scheme and* $(\mathsf{pubEval}, \mathsf{ctEval})$ *satisfies the homomorphic properties in lemma A.2, then the above construction has all-but-negligible probability to inverse correctly in the injective mode where the probability is taken over* $\mathsf{ABM.Gen}(1^\lambda)$.

Proof. Let $(\mathsf{ek}, \mathsf{ik}, \mathsf{tk})$ be the output of $\mathsf{ABM.Gen}(1^\lambda)$ as described in construction. Let $t = (t_\mathsf{c}, t_\mathsf{a}) \in \{0,1\}^{k_2} \times \{0,1\}^{k_1}$ be an injective tag, i.e. $\mathsf{PRF}(K, t_\mathsf{a}) \neq t_\mathsf{c}$, indicating that $\mathsf{RC}_t(K) = 1$. This formula and the homomorphic property of HE imply that ct is an HE encryption of $\mathsf{RC}_t(K)$, hence $C_{\mathsf{Dec}}(\mathsf{hdk}, \mathsf{ct}) = 1$. From lemma A.2, $\mathbf{A}_{\mathsf{pub}} = \mathbf{R}_{\mathsf{ct}} \cdot \mathbf{A} + \mathbf{G}$ and $\|R\|_\infty \leq 2 \cdot 4^d \beta m^2 (b-1)$ with overwhelming probability over the sampling of each $\mathbf{R}_{\mathbf{D}_i}$. Then $\mathbf{A}_1 = \mathbf{R} \cdot \mathbf{A} + \mathbf{G}$ with $\mathbf{R} = \mathbf{R}_{\mathsf{ct}} + \mathbf{R}_{\mathsf{ent}}$. It is easy to verify that $\mathbf{T}_{\bar{\mathbf{A}}} = (-\mathbf{R}, \mathbf{I}_m)$ is a gadget trapdoor of $\bar{\mathbf{A}}$ with norm $\|\mathbf{T}_{\bar{\mathbf{A}}}\| \leq 2 \cdot 4^d \beta m^2 (b-1) + mb^2 + 1$. From theorem 5.11, with sufficiently large $p \geq 2(b+1)(2 \cdot 4^d \beta m^2 (b-1) + mb^2 + 1) \geq 2(b+1)\|\mathbf{T}_{\bar{\mathbf{A}}}\|$, the LWR inversion algorithm recovers $s \in \mathbb{Z}_q^n$ from $\boldsymbol{y} = \lfloor \bar{\mathbf{A}} \boldsymbol{s} \rceil_p$ successfully. □

Lemma A.9 (l-Lossiness)**.** *Let $q > p^* \geq nmp\beta^*$, $\beta^* = m\beta(b^2 + 2 \cdot 4^d \beta m(b-1))$ and $n \geq 2\ell$, then our* ABM-LTF *construction has l-lossiness, where $l = (\ell + \lambda)\log q + n \log p^*$.*

Proof. This proof is similar to the proof of residual leakage of all-but-one LTF in [AKPW13, Theorem 7.3]. For any lossy tag $t \in \mathcal{T}_{\mathsf{loss}}$, in the algorithm $\mathsf{ABM.Eval}(\mathsf{ek}, t, \boldsymbol{s})$, we compute the image $\boldsymbol{y} = \lfloor \bar{\mathbf{A}} \cdot \boldsymbol{s} \rceil_p$ where $\bar{\mathbf{A}} = \begin{pmatrix} \mathbf{A} \\ \mathbf{RA} \end{pmatrix}$ and $\mathbf{A} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$. Next, we illustrate that we can regard $\bar{\mathbf{A}}$ as a lossy matrix from $\mathsf{Lossy}(1^n, 1^{2m}, 1^\ell, q, \chi^*)$ where χ^* is a β^*-bounded distribution over $\mathbb{Z}_q$.

We rewrite $\mathbf{A} = \mathbf{BC} + \mathbf{F}$ where $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m \times \ell}$, $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{\ell \times n}$ and $\mathbf{F} \xleftarrow{\$} \chi^{m \times n}$. Then, we rewrite $\bar{\mathbf{A}} = \bar{\mathbf{B}}\mathbf{C} + \bar{\mathbf{F}}$ where $\bar{\mathbf{B}} = \begin{pmatrix} \mathbf{B} \\ \mathbf{RB} \end{pmatrix}$ and $\bar{\mathbf{F}} = \begin{pmatrix} \mathbf{F} \\ \mathbf{RF} \end{pmatrix}$. Since $\mathbf{R} = \mathbf{R}_{\mathsf{ent}} + \mathbf{R}_{\mathsf{ct}}$ where $\mathbf{R}_{\mathsf{ent}} \xleftarrow{\$} [-b^2, b^2]^{m \times m}$ and $\mathbf{R}_{\mathsf{ct}}$ is coming from homomorphic computation. First, we need to prove that $(\mathbf{B}, \mathbf{RB})$ is statistically closed to the uniform distribution thanks to the randomness extractor $\mathbf{B}$. Though the detection of remaining entropy in $\mathbf{R}_{\mathsf{ct}}$ is hard, the source $\mathbf{R}_{\mathsf{ent}}$ can provide enough entropy for $\mathbf{R}$. For every row $\mathbf{r}^\top$ of $\mathbf{R}$, the term $\mathbf{RF}$ at most leaks $n \log q$ bits of information on $\mathbf{r}^\top$. Since $p_{\mathsf{min}} > b^2$ hence the remaining entropy in $\mathbf{r}$ is at least $m \log(2b^2) - n \log q > m + n \log q \geq 2\ell \log q + O(\lambda)$ with $m = kn$ and $b^k \geq q$. Therefore, the distribution $\bar{\mathbf{B}}$ is statistically closed to $U(\mathbb{Z}_q^{2m \times \ell})$. The next goal is to prove that every entry of $\mathbf{RF}$ is bounded by β^*. From lemma A.2 and the

choose of $\mathbf{R}_{\mathsf{ent}}$, $\|\mathbf{R}\|_\infty \le 2\cdot 4^d\beta m^2(b-1)+mb^2$. Therefore, for every column $\mathbf{f}$ of $\mathbf{F}$, $\|\mathbf{Rf}\|_\infty \le \|\mathbf{R}\|_\infty\|\mathbf{f}\|_\infty \le m\beta(2\cdot 4^d\beta m(b-1)+b^2)=\beta^*$ and we can model $\bar{\mathbf{F}}$ as a β^*-bounded distribution.

Finally, we apply the parameters $m^*=2m$ and β^* to lemma 4.3 to get the lossiness $l=(\ell+\lambda)\log q+n\log p^*$. □

Lemma A.10 (Indistinguishability)**.** *Assume* $\mathsf{LWE}_{\ell,m,q,\chi}$ *and* $\mathsf{HNFLWE}_{n,n,q,\chi}$ *is hard,* PRF *is a secure pseudorandom function scheme and* HE *has* IND-CPA *security. The above* ABM-LTF *construction has indistinguishability.*

Proof. This proof is similar to the proof of indistinguishability of the ABM-LTF scheme from Libert et al. [LSSS17, Lemma 14].

$\mathcal{A}$ is a PPT adversary to attack the indistinguishability property. We prove this theorem by hybrid arguments and the first game is the real indistinguishability game. Denote W_i as the event that adversary $\mathcal{A}$ outputs 1 in hybrid i.

Hybrid 0: This hyrbid is the experiment 0 in the indistinguishability game defined in A.1. The challenger generates the evaluation key ek as described in the ABM construction and gives ek to the adversary. The challenger answers each lossy tag queries by $\mathsf{ABM.LTag}(\mathsf{tk},\cdot)$.

Hybrid 1: This hybrid is the same as hybrid 0 except that the challenger generates the evaluation key ek in a different way. Instead of applying the Lossy function to generate $\mathbf{A}$ i.e. $\mathbf{A}\leftarrow\mathsf{Lossy}(1^n,1^m,1^\ell,q)$, the challenger samples $\mathbf{A}$ uniformly random on $\mathbb{Z}_q^{m\times n}$ i.e. $\mathbf{A}\xleftarrow{\$}\mathbb{Z}_q^{m\times n}$. From lemma 4.2, under the hardness of $\mathsf{LWE}_{\ell,m,q,\chi}$, the lossy matrix and the uniform matrix are computationally indistinguishable, hence $|\Pr[\mathsf{W}_0]-\Pr[\mathsf{W}_1]|\le n\mathsf{Adv}^{\ell,m,q,\chi}_{\mathsf{LWE},\mathcal{A}_0}(\lambda)$ for some LWE indistinguisher $\mathcal{A}_0$.

Hybrid 2: This hybrid is the same as hybrid 1 except that the challenger samples $\{\mathbf{D}_i\}_{i\in[g]}$ in uniformly at random i.e. $\mathbf{D}_i\xleftarrow{\$}\mathbb{Z}_q^{m\times m}$ for all $i\in[g]$, instead of making each $\mathbf{D}_i$ be a GSW encoding of the bit hdk_i. From lemma 5.10, under the hardness of $\mathsf{HNFLWE}_{n,n,q,\chi}$ and $m=kn\ge 2n+\omega(\log\lambda\cdot\log\log\lambda)$, we obtain that $|\Pr[\mathsf{W}_1]-\Pr[\mathsf{W}_2]|\le mg\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_1}(\lambda)$ for some adversary $\mathcal{A}_1$ attacking the pseudorandomness in lemma 5.10.

Hybrid 3: This hybrid is the same as hybrid 2 except that the challenger encrypts k_0 bits of 0 by HE, i.e. $d_i\leftarrow\mathsf{HE.Enc}(\mathsf{hek},0)$ for $i\in[k_0]$, instead of encrypting each bit of the PRF key K. From the IND-CPA security of HE, $|\Pr[\mathsf{W}_2]-\Pr[\mathsf{W}_3]|\le k_0\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HE},\mathcal{A}_2}(\lambda)$ for some CPA security attacker $\mathcal{A}_2$ of HE.

Hybrid 4: This hybrid is the same as hybrid 3 except that the challenger answers the lossy tag queries by $O_{\mathcal{T}_\mathsf{c}}(\cdot)$, an oracle that returns a uniform random core tag $t_\mathsf{c}\xleftarrow{\$}\mathcal{T}_\mathsf{c}$, which substitute the oracle $\mathsf{ABM.LTag}(\mathsf{tk},\cdot)$.

Next, we prove that for a secure PRF, the views of $\mathcal{A}$ in Hybrid 3 and Hybrid 4 are computationally indistinguishable. We can use distinguishing ability in Hybrid 3 and Hybrid 4 of $\mathcal{A}$ to construct a PRF attacker $\mathcal{A}_3$. In detail, $\mathcal{A}_3$ interacts with a PRF challenger C that uniformly choose a PRF key $K\xleftarrow{\$}\{0,1\}^{k_0}$ and answer each query $\mathsf{M}\in\{0,1\}^{k_1}$ by returning either $\mathsf{PRF}_K(\mathsf{M})$ or implementing a random function $R(\cdot)$ by lazy sampling and outputting $R(\mathsf{M})$. Initially, $\mathcal{A}_3$ generates the evaluation key $\mathsf{ek}=(\mathbf{A},\mathbf{A}_{\mathsf{ent}},\{d_i\}_{i\in[k_0]},\{\mathbf{D}_i\}_{i\in[g]},\mathsf{hek},\mathsf{hevk})$ by sampling $\mathbf{A}\xleftarrow{\$}\mathbb{Z}_q^{m\times n}$, $\mathbf{R}_{\mathsf{ent}}\xleftarrow{\$}[-b^2,b^2]^{m\times m}$, $(\mathsf{hek},\mathsf{hevk},\mathsf{hdk})\leftarrow\mathsf{HE.KeyGen}(1^\lambda)$, $d_i\xleftarrow{\$}\mathsf{HE.Enc}(\mathsf{hek},0)$ for $i\in[k_0]$, $\mathbf{D}_i\xleftarrow{\$}\mathbb{Z}_q^{m\times n}$ for $i\in[g]$ and computing $\mathbf{A}_{\mathsf{ent}}\leftarrow\mathbf{R}_{\mathsf{ent}}\mathbf{A}$. Then $\mathcal{A}_3$ gives ek to $\mathcal{A}$ and if $\mathcal{A}$ makes a lossy tag query for auxiliary tag $t_\mathsf{a}\in\{0,1\}^{k_1}$, $\mathcal{A}_3$ makes a PRF query for image t_a to C and returns the result to $\mathcal{A}$. If C uses $\mathsf{PRF}_K(\cdot)$ (resp. $R(\cdot)$) to answer queries, then $\mathcal{A}_3$ perfectly simulate the environment of Hybrid 3 (resp. 4) for $\mathcal{A}$. Therefore, $|\Pr[\mathsf{W}_3]-\Pr[\mathsf{W}_4]|\le\mathsf{Adv}_{\mathsf{PRF},\mathcal{A}_3}(\lambda)$.

Hybrid 5: This hybrid is the same as hybrid 4 except that the challenger encrypts each bit of the PRF key K, i.e. $d_i \leftarrow \mathsf{HE.Enc}(\mathsf{hek}, K_i)$, instead of encrypting k_0 bits of 0. From the IND-CPA security of HE, $|\Pr[\mathsf{W}_4] - \Pr[\mathsf{W}_5]| \leq k_0 \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HE},\mathcal{A}_2}(\lambda)$ for some CPA security attacker $\mathcal{A}_2$ of HE.

Hybrid 6: This hybrid is the same as hybrid 5 except that the challenger makes each $\mathbf{D}_i$ as a GSW encoding of hdk_i instead of sample each $\mathbf{D}_i$ uniformly at random. With similar arguments for transformation from Hybrid 1 to Hybrid 2, we obtain that $|\Pr[\mathsf{W}_5] - \Pr[\mathsf{W}_6]| \leq mg\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_1}(\lambda)$ for some adversary $\mathcal{A}_1$ attacking the pseudorandomness in lemma 5.10.

Hybrid 7: This hybrid is the same as hybrid 6 except that the challenger samples the public matrix $\mathbf{A}$ by the Lossy function i.e. $\mathbf{A} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q)$, instead of sample it uniformly random from $\mathbb{Z}_q^{m\times n}$. This hybrid is exactly the experiment 1 of the indistinguishability game. From lemma 4.2, $|\Pr[\mathsf{W}_0] - \Pr[\mathsf{W}_1]| \leq n\mathsf{Adv}^{\ell,m,q,\chi}_{\mathsf{LWE},\mathcal{A}_0}(\lambda)$ for some LWE indistinguisher $\mathcal{A}_0$.

Therefore, we obtain that

$$\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{ABM},\mathcal{A}}(\lambda) \leq 2n\mathsf{Adv}^{\ell,m,q,\chi}_{\mathsf{LWE},\mathcal{A}_0}(\lambda) + 2mg\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_1}(\lambda) + 2k_0\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HE},\mathcal{A}_2}(\lambda) + \mathsf{Adv}_{\mathsf{PRF},\mathcal{A}_3}(\lambda)$$

which is negligible in λ. □

Lemma A.11 (Evasiveness)**.** *Assuming the hardness of* $\mathsf{LWE}_{\ell,m,q,\chi}$ *and* $\mathsf{HNFLWE}_{n,n,q,\chi}$*, the* IND-CPA *security of* HE*, and the pseudorandomness of* PRF*, our* ABM-LTF *construction has evasiveness.*

Proof. This proof is similar to the proof of evasiveness of the ABM-LTF scheme from Libert et al. [LSSS17, Lemma 13].

$\mathcal{A}$ is a PPT adversary to attack the evasiveness property. We prove this lemma also by hybrid games and the first game is the real evasiveness game. We denote W_i as the event that adversary outputs 1 in hybrid i.

Hybrid 0: This hybrid is the real evasiveness game defined in A.1. The challenger gives the real evaluation key ek to the adversary $\mathcal{A}$, then A request for the following two types of queries:

1. $\mathsf{ABM.LTag}(\mathsf{tk}, \cdot)$: $\mathcal{A}$ submits an auxiliary tag t_a and get the corresponding $\mathsf{c} \leftarrow \mathsf{PRF}(K, \mathsf{a})$ returned. $\mathcal{A}$ asks this type of query for Q_1 times.

2. $\mathsf{isLossy}(\mathsf{tk}, \cdot)$: $\mathcal{A}$ submits a tag $t = (t_\mathsf{c}, t_\mathsf{a})$ and get the boolean value indicating whether $t_\mathsf{c} = \mathsf{PRF}(K, t_\mathsf{a})$ or not. $\mathcal{A}$ asks this type of query for Q_2 times.

Finally, $\mathcal{A}$ submits a challenge tag $t^* = (t^*_\mathsf{c}, t^*_\mathsf{a})$. $\mathcal{A}$ wins if and only if $t^* \in \mathcal{T}_{\mathsf{loss}}$ and $\mathcal{A}$ never obtained t^*_c by an oracle query t^*_a.

Hybrid 1: This hybrid is the same as hybrid 0 except that the challenger generates the evaluation key ek in a different way. Instead of applying the Lossy function to generate $\mathbf{A}$ i.e. $\mathbf{A} \leftarrow \mathsf{Lossy}(1^n, 1^m, 1^\ell, q)$, the challenger samples $\mathbf{A}$ uniformly random on $\mathbb{Z}_q^{m\times n}$ i.e. $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$. From lemma 4.2, $|\Pr[\mathsf{W}_0] - \Pr[\mathsf{W}_1]| \leq n\mathsf{Adv}^{\ell,m,q,\chi}_{\mathsf{LWE},\mathcal{A}_0}(\lambda)$ for some LWE indistinguisher $\mathcal{A}_0$.

Hybrid 2: This hybrid is the same as hybrid 1 except that the challenger samples $\{\mathbf{D}_i\}_{i\in[g]}$ in uniformly at random i.e. $\mathbf{D}_i \xleftarrow{\$} \mathbb{Z}_q^{m\times m}$ for all $i \in [g]$, instead of making each $\mathbf{D}_i$ be a GSW encoding of the bit hdk_i. From lemma 5.10, under the hardness of $\mathsf{HNFLWE}_{n,n,q,\chi}$ and $m = kn \geq 2n + \omega(\log\lambda \cdot \log\log\lambda)$, we obtain that $|\Pr[\mathsf{W}_1] - \Pr[\mathsf{W}_2]| \leq mg\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_1}(\lambda)$ for some adversary $\mathcal{A}_1$ attacking the pseudorandomness in lemma 5.10.

Hybrid 3: This hybrid is the same as hybrid 2 except that the challenger encrypts k_0 bits of 0 by HE, i.e. $d_i \leftarrow \mathsf{HE.Enc}(\mathsf{hek}, 0)$, instead of encrypting each bit of the PRF key K. From the IND-CPA security of HE, $|\Pr[\mathsf{W}_2] - \Pr[\mathsf{W}_3]| \leq k_0\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HE},\mathcal{A}_2}(\lambda)$ for some CPA security attacker $\mathcal{A}_2$ of HE.

Hybrid 4: This hybrid is the same as hybrid 3 except that the challenger returns two queries in a different way. The challenger maintains a random function $R : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ by lazy sampling, and returns $t_c = R(t_a)$ instead of $t_c = \mathsf{PRF}(K, t_a)$ in the lossy core tag query, and returns the bit $t_c \stackrel{?}{=} R(t_a)$ if $\mathcal{A}$ makes a lossy tag judgement query for $t = (t_c, t_a)$. Since R is a random function, $\Pr[\mathsf{W}_4] = Q_2/2^{k_2(\lambda)}$.

Similarly to the proof of indistinguishability, we prove that for a secure PRF, the views of $\mathcal{A}$ in Hybrid 3 and Hybrid 4 are computationally indistinguishable. We construct a PRF attacker $\mathcal{A}_3$ based on the distinguihing ability in Hybrid 3 and Hybrid 4 of $\mathcal{A}$. In detail, $\mathcal{A}_3$ interacts with a PRF challenger C that uniformly choose a PRF key $K \xleftarrow{\$} \{0,1\}^{k_0}$ and answer each query $\mathsf{M} \in \{0,1\}^{k_1}$ by returning either $\mathsf{PRF}_K(\mathsf{M})$ or implementing a random function $R(\cdot)$ by lazy sampling and outputting $R(\mathsf{M})$. Initially, $\mathcal{A}_3$ generates the evaluation key $\mathsf{ek} = (\mathbf{A}, \mathbf{A}_{\mathsf{ent}}, \{d_i\}_{i\in[k_0]}, \{\mathbf{D}_i\}_{i\in[g]}, \mathsf{hek}, \mathsf{hevk})$ by sampling $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$, $\mathbf{R}_{\mathsf{ent}} \xleftarrow{\$} [-b^2, b^2]^{m\times m}$, $(\mathsf{hek}, \mathsf{hevk}, \mathsf{hdk}) \leftarrow \mathsf{HE.KeyGen}(1^\lambda)$, $d_i \xleftarrow{\$} \mathsf{HE.Enc}(\mathsf{hek}, 0)$ for $i \in [k_0]$, $\mathbf{D}_i \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$ for $i \in [g]$ and computing $\mathbf{A}_{\mathsf{ent}} \leftarrow \mathbf{R}_{\mathsf{ent}}\mathbf{A}$. Then $\mathcal{A}_3$ gives ek to $\mathcal{A}$. If $\mathcal{A}$ makes a lossy tag query for auxiliary tag $t_a \in \{0,1\}^{k_1}$, $\mathcal{A}_3$ makes a PRF query for image t_a and returns the result from C to $\mathcal{A}$. If $\mathcal{A}$ makes a lossy tag judgement query for tag $t = (t_c, t_a)$, $\mathcal{A}_3$ makes a PRF query for image t_a and returns 0/1 to $\mathcal{A}$, which indicates whether t_c matches the result from C or not. As a result, $\mathcal{A}_3$ makes $Q_1 + Q_2$ PRF queries. If C uses $\mathsf{PRF}_K(\cdot)$ (resp. $R(\cdot)$) to answer queries, then $\mathcal{A}_3$ perfectly simulate the environment of Hybrid 3 (resp. 4) for $\mathcal{A}$. Therefore, $|\Pr[\mathsf{W}_3] - \Pr[\mathsf{W}_4]| \le \mathsf{Adv}_{\mathsf{PRF},\mathcal{A}_3}(\lambda)$.

Finally, with the help of traingular inequality, we obtain that

$$\mathsf{Adv}^{\mathsf{EVA}}_{\mathsf{ABM},\mathcal{A}}(\lambda) \le n\mathsf{Adv}^{\ell,m,q,\chi}_{\mathsf{LWE},\mathcal{A}_0}(\lambda) + mg\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_1}(\lambda) + k_0\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HE},\mathcal{A}_2}(\lambda) + \mathsf{Adv}_{\mathsf{PRF},\mathcal{A}_3}(\lambda) + \frac{Q_2}{2^{k_2(\lambda)}}$$

which is negligible in λ. □

A.1 Deterministic Encryption

Deterministic public key encryption (DPKE) is a variant of PKE with deterministic encryption and decryption algorithm. The goal of this primitive is to guarantee the security if the plaintexts are drawn from a large min-entropy distribution. Here we give the definition that a deterministic encryption scheme requires the computational indistinguishability of plaintexts from two different high-entropy distributions.

Definition A.12. *A deterministic public key encryption scheme* DPKE *with message space $\mathcal{S} = \mathcal{S}_\lambda$ includes the following algorithms:*

- ***Key Generation.*** *A* PPT *algorithm* $\mathsf{DPKE.KeyGen}(1^\lambda)$ *generates a public and secret key pair* $(\mathsf{pk}, \mathsf{sk})$.
- ***Encryption.*** *A deterministic algorithm* $\mathsf{DPKE.Enc}(\mathsf{pk}, \boldsymbol{s})$ *takes a public key* pk *and a plaintext $\boldsymbol{s} \in \mathcal{S}$, and outputs the ciphertext $\boldsymbol{y}$.*
- ***Decryption.*** *A deterministic algorithm* $\mathsf{DPKE.Dec}(\mathsf{sk}, \boldsymbol{y})$ *takes a secret key* sk *and a ciphertext $\boldsymbol{y}$, and output the plaintext $\boldsymbol{s}$.*

We require DPKE *has the following properties:*

- ***Correctness.*** *For* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$*, we have* $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \boldsymbol{s}))$ *with overwhelming probability over randomness of* KeyGen.

- $k(\lambda)$-***Security.*** *Let $\mathcal{S}_0$ and $\mathcal{S}_1$ be any two distributions over $\mathcal{M}^\lambda$ which are efficiently samplable in* $\mathsf{poly}(\lambda)$ *time with min-entropy $H_\infty^{\mathsf{smooth}}(\mathcal{S}_0) \geq k$ and $H_\infty^{\mathsf{smooth}}(\mathcal{S}_1) \geq k$, then for all* PPT *adversary $\mathcal{A}$,*

$$\mathsf{Adv}^{k(\lambda)}_{\mathsf{DPKE},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}(1^\lambda, \mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \boldsymbol{s}_0)) = 1\right] - \Pr\left[\mathcal{A}(1^\lambda, \mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \boldsymbol{s}_1)) = 1\right]\right|$$

is negligible, where the probability is taken over $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$, $\boldsymbol{s}_0 \xleftarrow{\$} \mathcal{S}_0$ *and* $\boldsymbol{s}_1 \xleftarrow{\$} \mathcal{S}_1$.

We adopt the construction of DPKE from [AKPW13], except for some parameter change. In [AKPW13], the security of DPKE requires the message distribution $\mathcal{S}$ to be bounded, e.g. binary vectors, while we remove the bound limitation. Since we proved the hardness of entropic LWR in 4.3 for any secret distirbution $\mathcal{S}$ over $\mathbb{Z}_q^n$ with high min-entropy, we can change the message space to be $\mathbb{Z}_q^n$ instead of $\{0,1\}^n$.

Construction A.13. *Let λ be a security parameter, and $n, m, p, q = \mathsf{poly}(\lambda)$ be lattice parameters. Let b be a gadget base. Let $\mathcal{S}$ be an entropic distribution over $\mathbb{Z}_q^n$ such that* $\Pr[\boldsymbol{s} \notin (\mathbb{Z}_q^n)^* : \boldsymbol{s} \leftarrow \mathcal{S}]$ *is negligible. Our* DPKE *scheme includes the following algorithms:*

- $\mathsf{KeyGen}(1^\lambda)$: Sample $(\mathbf{A}, \mathbf{T_A}) \leftarrow \mathsf{TrapGen}(1^n, q, b)$. Output $\mathsf{pk} = \mathbf{A}$ and $\mathsf{sk} = (\mathbf{A}, \mathbf{T_A})$.
- $\mathsf{Enc}(\mathsf{pk}, \boldsymbol{s})$: Input public key $\mathsf{pk} = \mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and a plaintext $\boldsymbol{s} \leftarrow \mathcal{S}$, output $\lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_p$.
- $\mathsf{Dec}(\mathsf{sk}, \boldsymbol{y})$: Input secret key $\mathsf{sk} = (\mathbf{A}, \mathbf{T_A})$ and a ciphertext $\boldsymbol{y} \in \mathbb{Z}_p^m$, run the LWR inversion algorithm to return the plaintext $\boldsymbol{s} \leftarrow \mathsf{LWRInvert}(\mathbf{T_A}, \mathbf{A}, \boldsymbol{y})$.

Theorem A.14. *Let q be a prime and χ be a β-bounded distribution over $\mathbb{Z}_q$ such that $q > p^* \geq nmp\beta$ and $p \geq 2(b+1)(2n\beta+1)$. Assuming the hardness of* $\mathsf{HNFLWE}_{n,n,q,\chi}$ *and* $\mathsf{LWE}_{\ell,m,q,\chi}$*, our* DPKE *scheme has k-security for $k = n \log p^* + (\ell + \lambda + 1)\log q + \omega(\log \lambda)$.*

Proof. Correctness follows the same way of LTF correctness proof in lemma 5.17.

The proof of k-security is similar to [AKPW13, Theorem 8.2]. From lemma 4.3, the hardness of $\mathsf{LWE}_{\ell,m,q,\chi}$ implies the hardness of $\mathsf{ent\text{-}dLWR}(q, p, n, m, \mathcal{S})$ for entropic distribution $\mathcal{S}$ over $\mathbb{Z}_q^n$ such that $H_\infty^{\mathsf{smooth}}(\mathcal{S}) \geq k = n \log p^* + (\ell + \lambda + 1)\log q + \omega(\log \lambda)$. Let $\mathcal{S}_0$ and $\mathcal{S}_1$ be two distributions with smooth min-entropy at least k. With the hardness of $\mathsf{HNFLWE}_{n,n,q,\chi}$, we have the following distributions computationally indistinguishable:

$$(\mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s}_0 \rceil_p) \overset{c}{\approx} (\bar{\mathbf{A}}, \lfloor \bar{\mathbf{A}} \cdot \boldsymbol{s}_0 \rceil_p) \overset{c}{\approx} (\bar{\mathbf{A}}, \lfloor \mathbf{u} \rceil_p) \overset{c}{\approx} (\bar{\mathbf{A}}, \lfloor \bar{\mathbf{A}} \cdot \boldsymbol{s}_1 \rceil_p) \overset{c}{\approx} (\mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s}_1 \rceil_p)$$

where $\mathbf{A}$ comes from the first term in $\mathsf{TrapGen}(1^\lambda, q, b)$, $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\boldsymbol{s}_0 \leftarrow \mathcal{S}_0$ and $\boldsymbol{s}_1 \leftarrow \mathcal{S}_1$. Therefore, we obtain the advantage of a PPT adversary $\mathcal{A}$ in attacking k-security:

$$\mathsf{Adv}^{k(\lambda)}_{\mathsf{DPKE},\mathcal{A}}(\lambda) \leq 2m\mathsf{Adv}^{n,m,q}_{\mathsf{pse},\mathcal{A}_0}(\lambda) + 2\mathsf{Adv}^{n,m,q,p,k}_{\mathsf{ent\text{-}dGLWR},\mathcal{A}_1}(\lambda)$$

which is negligible. □

A.2 Public Key Encryption with Selective Opening Security

In this appendix section, we recall some notions of cryptography primitives with the standard security model which we used in our LTF and ABM construction.

Public Key Encryption. A PKE scheme with message space $\mathcal{M} = \mathcal{M}_\lambda$ consists of the following three PPT algorithms:

- $\mathsf{PKE.Gen}(1^\lambda)$: Input the security parameter and output a public key pk and a secret key sk.
- $\mathsf{PKE.Enc}(\mathsf{pk}, \mathsf{msg})$: Input a public key pk and a message $\mathsf{msg} \in \mathcal{M}$, and output a ciphertext ct.
- $\mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{ct})$: Input a secret key sk and a ciphertext ct, and output a message $\mathsf{msg} \in \mathcal{M}$ or $\perp$.

The correctness refers to that for all message msg, for $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\lambda)$, $\mathsf{PKE.Dec}(\mathsf{sk}, \mathsf{PKE.Enc}(\mathsf{pk}, \mathsf{msg})) = m$ holds overwhelmingly where the probability is taken from the randomness in $\mathsf{PKE.Gen}$ and $\mathsf{PKE.Enc}$.

We adopt the following definitions related to efficiently samplable, explainable and re-samplable from [Hof12].

Definition A.15 (Efficiently samplable and explainable)**.** *A discrete distribution $\mathcal{S}$ is efficiently samplable and explainable if every element $\mathbf{s}$ can be explained by sampling from a uniform randomness R. There exists* PPT *algorithm $\mathsf{Samp}_\mathcal{S}$ and $\mathsf{Expl}_\mathcal{S}$ satisfying that*

1. *$\mathsf{Samp}_\mathcal{S}(1^k; R)$ where $R \xleftarrow{\$} \{0,1\}^{|R|}$ samples exactly from $\mathcal{S}$;*
2. *For all $\mathbf{s} \in \mathcal{S}$, $\mathsf{Expl}_\mathcal{S}(\mathbf{s})$ returns randomness R such that $s = \mathsf{Samp}_\mathcal{S}(1^k; R)$.*

Definition A.16 (Efficiently re-samplable)**.** *Let $N = N(\lambda) > 0$ and $n = n(\lambda)$. A joint distribution* dist *over $(\{0,1\}^n)^N$ is efficiently re-samplable, if ther exists a* PPT *algorithm $\mathsf{ReSamp}_{\mathsf{dist}}$ such that for all $\mathcal{I} \subseteq [N]$ and any partial vector $\mathbf{msg}'_\mathcal{I} := (\mathsf{msg}'_i)_{i \in \mathcal{I}} \in (\{0,1\}^n)^{|\mathcal{I}|}$, $\mathsf{ReSamp}_{\mathsf{dist}}(\mathbf{msg}'_\mathcal{I})$ samples from* dist *conditioned on $\mathsf{msg}_i = \mathsf{msg}'_i$ for $i \in \mathcal{I}$.*

IND-SO-CCA Security. We first recall the following experiment $\mathsf{Exp}^{\mathsf{IND\text{-}SO\text{-}CCA}}_{\mathsf{PKE},\mathcal{A},N,b}$ between a challenger C and an adversary $\mathcal{A}$ for $b \in \{0,1\}$ and polynomial $N = N(\lambda)$.

1. At the beginning, C runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\lambda)$ and sends pk to $\mathcal{A}$;
2. $\mathcal{A}$ is given 1^λ and pk as input and an oracle to $\mathsf{PKE.Dec}(\mathsf{sk}, \cdot)$, chooses an efficiently samplable, explainable and re-samplable joint distribution dist over $\mathcal{M}^N$, and sends dist to C;
3. C samples $\mathbf{msg}_0 := (\mathsf{msg}_i)_{i \in [N]} \xleftarrow{\$} \mathsf{dist}$ and $\mathbf{R} := (R_i)_{i \in [N]} \xleftarrow{\$} (\mathcal{R}_{\mathsf{PKE.Enc}})^N$ where $\mathcal{R}_{\mathsf{PKE.Enc}}$ refers to the randomness space in $\mathsf{PKE.Enc}$. Then C computes $\mathbf{C} := (\mathsf{ct}_i)_{i \in [N]} \leftarrow (\mathsf{PKE.Enc}(\mathsf{pk}, \mathsf{msg}_i; R_i))_{i \in [N]}$ and sends all ciphertexts $\mathbf{C}$ to $\mathcal{A}$;
4. $\mathcal{A}$ is given $\mathbf{C}$ as input and an oracle to $\mathsf{PKE.Dec}(\mathsf{sk}, \cdot)$, selects a subset $\mathcal{I} \in [N]$ and sends $\mathcal{I}$ to C;
5. C re-samples $\mathbf{msg}_1$ from dist conditioned on $(\mathsf{msg}_i)_{i \in \mathcal{I}}$ and sends $(\mathsf{msg}_i, R_i)_{i \in \mathcal{I}}$ and $\mathbf{msg}_b$ to $\mathcal{A}$;
6. $\mathcal{A}$ is given $(\mathsf{msg}_i, R_i)_{i \in \mathcal{I}}$ and $\mathbf{msg}_b$ as input and the decryption oracle $\mathsf{PKE.Dec}(\mathsf{sk}, \cdot)$, finally outputs a bit $b' \in \{0,1\}$;

We require that $\mathcal{A}$ never submits a received challenge ciphertext ct_i to the decryption oracle. We say that if a PKE scheme has IND-SO-CCA security if for all PPT adversary $\mathcal{A}$ and polynomial N,

$$\mathsf{Adv}^{\mathsf{IND\text{-}SO\text{-}CCA}}_{\mathsf{PKE},\mathcal{A},N}(\lambda) := \left| \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}SO\text{-}CCA}}_{\mathsf{PKE},\mathcal{A},N,0}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}SO\text{-}CCA}}_{\mathsf{PKE},\mathcal{A},N,1}(\lambda) = 1\right] \right|$$

is negligible.

Lossy Authenticated Encryption. A LAE scheme with key space $\{0,1\}^{2k}$ and message space $\{0,1\}^k$ for $k = k(\lambda)$ consists of the following two PPT algorithms:

- $\mathsf{E}(K, \mathsf{msg})$: Input a secret key $K \in \{0,1\}^{2k}$ and a message $\mathsf{msg} \in \{0,1\}^k$, output a ciphertext ct.
- $\mathsf{D}(K, \mathsf{ct})$: Input a secret key $K \in \{0,1\}^{2k}$ and a ciphertext ct, output a message $\mathsf{msg} \in \{0,1\}^k$ or a decryption failure symbol $\perp$.

We consider the following properties:

- **Correctness.** $\mathsf{D}(K, \mathsf{E}(K, \mathsf{msg})) = \mathsf{msg}$ holds for all $K \in \{0,1\}^{2k}$ and $\mathsf{msg} \in \{0,1\}^k$.
- **Authentication.** This security notion is defined by the following game between a challenger C and an adversary $\mathcal{A}$.

  1. At the beginning of the game, C samples a uniform key $K \xleftarrow{\$} \{0,1\}^{2k}$;
  2. **One Time Encryption Query.** $\mathcal{A}$ is given 1^λ as input, chooses and sends a message $\mathsf{msg} \in \{0,1\}$ to C, and get the ciphertext $\mathsf{ct} \leftarrow \mathsf{E}(K, \mathsf{msg})$ from C.
  3. **Many Times Decryption Query.** $\mathcal{A}$ queries for the decryption of a ciphertext ct through a decryption oracle $\mathsf{D}(K, \cdot)$ polynomial times.
  4. $\mathcal{A}$ wins if $\mathcal{A}$ outputs a valid ciphertext $\mathsf{ct}^* \neq \mathsf{ct}$, i.e. $\mathsf{D}(K, \mathsf{ct}^*) \neq \perp$.

  We require that the probability of winning the game for every PPT adversary $\mathcal{A}$ is negligible.

- **Lossiness.** For message $\mathsf{msg} \in \{0,1\}^k$, let $\mathcal{D}_{\mathsf{msg}}$ be the distribution $\mathsf{E}(K, \mathsf{msg})$ where $K \xleftarrow{\$} \{0,1\}^{2k}$. For any $\mathsf{msg}_0, \mathsf{msg}_1 \in \{0,1\}^k$, the two distributions $\mathcal{D}_{\mathsf{msg}_0}$ and $\mathcal{D}_{\mathsf{msg}_1}$ are identical.

Universal Hash Function. Let $\mathcal{UH} \subseteq \{h : \{0,1\}^L \to \{0,1\}^t\}$ be a family of universal hash function, then for any distinct $x_1, x_2 \in \{0,1\}^L$, we have

$$\Pr_{h \xleftarrow{\$} \mathcal{UH}}[h(x_1) = h(x_2)] \leq 2^{-t}.$$

Lemma A.17 (Leftover Hash Lemma)**.** *For any integers $d \leq k \leq l$, let $\mathcal{UH} \subseteq \{h : \{0,1\}^l \to \{0,1\}^{k-d}\}$ be a family of universal hash functions. Then, for any random distribution $\mathcal{X}$ over $\{0,1\}^l$ such that $H_\infty(X) \geq k$, we have*

$$\mathsf{SD}(h(\mathcal{X}), U(\{0,1\}^{k-d}) \mid h)_{h \xleftarrow{\$} \mathcal{UH}} \leq 2^{-\frac{d}{2}-1}.$$

Our compact LTF and ABM-LTF can be adapted to the black box construction of PKE scheme with SO-CCA in [Hof12]. Next, we present the construction from Hofheinz [Hof12]. We require the following ingredients:

- A lossy trapdoor function $\mathsf{LTF} = (\mathsf{LTF.IGen}, \mathsf{LTF.LGen}, \mathsf{LTF.Eval}, \mathsf{LTF.Invert})$ with domain $\{0,1\}^L$ and lossiness l_0;
- An all-but-many lossy trapdoor function $\mathsf{ABM} = (\mathsf{ABM.Gen}, \mathsf{ABM.Eval}, \mathsf{ABM.Invert}, \mathsf{ABM.LTag})$ with domain $\{0,1\}^L$ and lossiness l_1;

- A universal hash function family $\mathcal{UH} = \mathcal{UH}_\lambda$ with UHF $h : \{0,1\}^L \to \{0,1\}^{2k}$ for some $n = n(\lambda)$ and $k = k(\lambda)$ such that $L - l_0 - l_1 - 2k = \omega(\log\lambda)$.
- A lossy authenticated encryption scheme $\mathsf{LAE} = (\mathsf{E}, \mathsf{D})$ with key $K \in \{0,1\}^{2k}$, message $m \in \{0,1\}^k$ and ciphertext $\mathsf{ct} \in \{0,1\}^{2\kappa}$.

With the cryptography primitives above, we have the following $\mathsf{PKE} = (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ scheme.

- $\mathsf{PKE.Gen}(1^\lambda)$:
  1. Sample $(\mathsf{ek}_0, \mathsf{ik}_0) \leftarrow \mathsf{LTF.IGen}(1^\lambda)$, $(\mathsf{ek}_1, \mathsf{ik}_1, \mathsf{tk}) \leftarrow \mathsf{ABM.Gen}(1^\lambda)$ and $h \xleftarrow{\$} \mathcal{UH}$;
  2. Output $\mathsf{pk} := (\mathsf{ek}_0, \mathsf{ek}_1, h)$ and $\mathsf{sk} := (\mathsf{ik}_0, \mathsf{ek}_1, h)$;
- $\mathsf{PKE.Enc}(\mathsf{pk}, m)$: Input $\mathsf{pk} = (\mathsf{ek}_0, \mathsf{ek}_1, h)$ and a message $m \in \{0,1\}^k$.
  1. Sample $\boldsymbol{s} \xleftarrow{\$} \{0,1\}^L$ and compute the LAE key $K \leftarrow h(x)$;
  2. Encrypt m by the LAE scheme $\mathsf{ct} \leftarrow \mathsf{E}(K, m)$;
  3. Compute $\boldsymbol{y}_0 \leftarrow \mathsf{LTF.Eval}(\mathsf{ek}_0, x)$ and $\boldsymbol{y}_1 \leftarrow \mathsf{ABM.Eval}(\mathsf{ek}_1, (t_\mathsf{c}, \boldsymbol{y}_0), x)$ where $t_\mathsf{c} \leftarrow \mathsf{Samp}_{\mathcal{T}_\mathsf{core}}(1^\lambda; R_{t_\mathsf{c}})$;
  4. Output $C := (\mathsf{ct}, \boldsymbol{y}_0, t_\mathsf{c}, \boldsymbol{y}_1)$.

  Notice that the randomness in $\mathsf{PKE.Enc}$ is $(\boldsymbol{s}, R_{t_\mathsf{c}})$.
- $\mathsf{PKE.Dec}(\mathsf{sk}, C)$: Input $\mathsf{sk} = (\mathsf{ik}, \mathsf{ek}, h)$ and $C = (\mathsf{ct}, \boldsymbol{y}_0, t_\mathsf{c}, \boldsymbol{y}_1)$.
  1. Compute $\boldsymbol{s} \leftarrow \mathsf{LTF.Invert}(\mathsf{ik}_0, \boldsymbol{y}_0)$;
  2. If $\boldsymbol{y}_1 \neq \mathsf{ABM.Eval}(\mathsf{ek}_1, (t_\mathsf{c}, \boldsymbol{y}_0))$, return $\perp$;
  3. Compute $K \leftarrow h(x)$ and output $m \leftarrow \mathsf{D}(K, \mathsf{ct})$.

The proof of IND-SO-CCA security is already done in [Hof12] and [HHK+24], so we omit it here.

For a post-quantum instantiation of the PKE scheme with IND-SO-CCA security, we choose the LTF and ABM scheme to be our l_0-LTF from Construction 5.14 and l_1-ABM-LTF from Construction A.5 with same preimage space $\mathbb{Z}_q^n$. Apart from the inner constraints of LTF and ABM-LTF, we need $n\log q - l_0 - l_1 - 2k = \omega(\log\lambda)$. Therefore, with the compact expansion property of our LTF and ABM-LTF, we can obtain a SO-CCA PKE scheme with compact expansion ($\frac{|\mathsf{ct}|}{|m|}$ is constant).

B Hardness of Entropic LWR from Noise Lossiness

In this part, we prove a lemma which is analogous to Lemma 4.3 via noise lossiness [BD20a].

Lemma B.1. *Let n, m, ℓ, p, q, β be positive integers and σ be a Gaussian parameter such that $q > nmp\beta(\sigma + 1)$, and χ be a β-bounded distribution over $\mathbb{Z}_q$. Let $(\boldsymbol{s}, \mathsf{aux})$ be a pair of correlated random variables with $\boldsymbol{s}$ distributed according to some distribution $\mathcal{S} \subseteq \mathbb{Z}_q^n$ and $\Pr_{\boldsymbol{s}}\left[\boldsymbol{s} \notin \left(\mathbb{Z}_q^n\right)^*\right] < \delta$, and let $\tilde{\mathbf{A}}$ be a matrix independently output by the algorithm $\mathsf{Lossy}(1^n, 1^m, 1^\ell, q, \chi)$. Let the random variable $\boldsymbol{e}$ be sampled from the continuous Gaussian distribution D_σ^n. Then for $\varepsilon = 2^{-\lambda} + \delta + 2^{-\ell+1} + e^{-\left(\frac{\pi}{4} - \ln 2\right)n}$, any $\varepsilon' > 0$ and any every function f taken input over $\mathcal{S}$, we have:*

$$H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \left\lfloor \tilde{\mathbf{A}} \cdot \boldsymbol{s} \right\rceil_p, \mathsf{aux}\right) \geq H_\infty^{\varepsilon'}\left(f(\boldsymbol{s}) \mid \boldsymbol{s} + \boldsymbol{e}, \mathsf{aux}\right) - (\ell + \lambda)\log q.$$

Proof. According to Definition 4.1, $\tilde{\mathbf{A}}$ can be written as $\tilde{\mathbf{A}} = \mathbf{B}\cdot\mathbf{C}+\mathbf{F}$, then $\lfloor \tilde{\mathbf{A}}\cdot \boldsymbol{s}\rceil_p = \lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s}+\mathbf{F}\cdot\boldsymbol{s}\rceil_p$. Furthermore, $\lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s}+\mathbf{F}\cdot\boldsymbol{s}\rceil_p$ can be written as

$$\lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s}+\mathbf{F}\cdot\boldsymbol{s}\rceil_p = \lfloor \mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s}+\mathbf{F}\cdot(\boldsymbol{s}+\lfloor \boldsymbol{e}\rceil)-\mathbf{F}\cdot\lfloor \boldsymbol{e}\rceil\rceil_p .$$

We define the set $I \stackrel{\text{def}}{=} \left\{ i\in[m] : \lfloor (\mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s}+\mathbf{F}\cdot(\boldsymbol{s}+\lfloor \boldsymbol{e}\rceil))_i\rceil_p \neq \left\lfloor \left(\tilde{\mathbf{A}}\cdot\boldsymbol{s}\right)_i\right\rceil_p \right\}$, where $(\boldsymbol{x})_i[j]$ denotes the jth coefficient of ith coordinate of $\boldsymbol{x}$ relative to $\mathbf{B}$. Let $Z = \left\{ \left(i, \left\lfloor \left(\tilde{\mathbf{A}}\cdot\boldsymbol{s}\right)_i\right\rceil_p\right) : i\in I\right\}$, and it is not hard to see that $(\tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_{\mathbf{B},p})$ can be reconstructed completely via $\mathbf{B},\mathbf{C},\mathbf{F},\mathbf{C}\boldsymbol{s},\boldsymbol{s}+\lfloor \boldsymbol{e}\rceil, Z$. Therefore:

$$H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \left\lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s}\right\rceil_p, \mathsf{aux}\right) \geq H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \mathbf{B},\mathbf{C},\mathbf{F},\mathbf{C}\boldsymbol{s},\boldsymbol{s}+\lfloor \boldsymbol{e}\rceil, Z, \mathsf{aux}\right).$$

Next we show a lower bound for the right hand side by bounding the min-entropy loss given Z. To do this, we first bound the probability that the size of I is large:

Claim B.2. $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[|I|>\lambda] < \delta + 2^{-\ell+1} + 2^{-\lambda} + e^{-\left(\frac{\pi}{4}-\ln 2\right)n}$.

Proof. We first separate the event $|I|>\lambda$ into two conditions: $\|\boldsymbol{e}\|_1 \leq n\sigma/2$ and $\|\boldsymbol{e}\|_1 > n\sigma/2$ and get:

$$\begin{aligned}
\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I|>\lambda\ ] &= \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I|>\lambda \mid \|\boldsymbol{e}\|_1 > n\sigma/2\ ]\cdot \Pr_{\boldsymbol{e}}[\ \|\boldsymbol{e}\|_1 > n\sigma/2\ ] \\
&\quad + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I|>\lambda \mid \|\boldsymbol{e}\|_1 \leq n\sigma/2\ ]\cdot \Pr_{\boldsymbol{e}}[\ \|\boldsymbol{e}\|_1 \leq n\sigma/2\ ] \\
&\leq \Pr_{\boldsymbol{e}}[\ \|\boldsymbol{e}\|_1 > n\sigma/2\ ] + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I|>\lambda \mid \|\boldsymbol{e}\|_1 \leq n\sigma/2\ ] \\
&\leq e^{-\left(\frac{\pi}{4}-\ln 2\right)n} + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I|>\lambda \mid \|\boldsymbol{e}\|_1 \leq n\sigma/2\ ] \qquad (13)
\end{aligned}$$

where the inequality (13) is taken from Lemma B.3 by setting $t = 1/2$.

Then we will find an upper bound of the latter term in (13). We fix $\boldsymbol{e}$ such that $\|\boldsymbol{e}\|_1 \leq n\sigma/2$ and we can also divide the event $|I|>\lambda$ into two conditions: $\boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*$ and $\boldsymbol{s}\notin\left(\mathbb{Z}_q^n\right)^*$ and obtain:

$$\begin{aligned}
\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}[\ |I|>\lambda\ ] &= \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[\ |I|>\lambda \mid \boldsymbol{s}\notin\left(\mathbb{Z}_q^n\right)^*\ \right]\cdot \Pr_{\boldsymbol{s}}\left[\ \boldsymbol{s}\notin\left(\mathbb{Z}_q^n\right)^*\ \right] \\
&\quad + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[\ |I|>\lambda \mid \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\ \right]\cdot \Pr_{\boldsymbol{s}}\left[\ \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\ \right] \qquad (14) \\
&\leq \Pr_{\boldsymbol{s}}\left[\ \boldsymbol{s}\notin\left(\mathbb{Z}_q^n\right)^*\ \right] + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[\ |I|>\lambda \mid \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\ \right].
\end{aligned}$$

Then, we have

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}[\ |I|>\lambda\ ] < \delta + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[\ |I|>\lambda \mid \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\ \right].$$

So our next step is to bound $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s}}\left[\ |I|>\lambda \mid \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\ \right]$.

For any $\boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*$ and independently chosen matrix $\mathbf{C}\xleftarrow{\$}\mathbb{Z}_q^{\ell\times n}$, $\mathbf{C}\cdot\boldsymbol{s}$ is uniformly distributed over $\mathbb{Z}_q^\ell$. Thus by the lower bound of $\left|(\mathbb{Z}_q^\ell)^*\right|$,

$$\Pr_{\mathbf{C},\boldsymbol{s}}\left[\mathbf{C}\cdot\boldsymbol{s}\in\left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s}\in\left(\mathbb{Z}_q^n\right)^*\right] \geq 1-2^{-\ell+1}.$$

Now we further divide $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right]$ into two cases as follows:

$$\begin{aligned}
&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \\
=&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C}\cdot\boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^*\right] \cdot \Pr_{\mathbf{C},s}\left[\mathbf{C}\cdot\boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] \\
+&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] \cdot \Pr_{\mathbf{C},s}\left[\mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right].
\end{aligned}$$

Combining the above equation with (1), we have

$$\begin{aligned}
&\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda\right] \\
&< \delta + \Pr_{\mathbf{C},s}\left[\mathbf{C}\cdot\boldsymbol{s} \notin \left(\mathbb{Z}_q^\ell\right)^* \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*\right] + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] \\
&< \delta + 2^{-\ell+1} + \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right].
\end{aligned} \tag{15}$$

It's easy to see

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*, \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right] = \Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right]$$

as $\mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*$ implies $\boldsymbol{s} \in \left(\mathbb{Z}_q^n\right)^*$, so it's remain to bound $\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},s}\left[|I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*\right]$. To do this, we denote the i-th column of the matrices $\mathbf{B}$ and $\mathbf{F}$ as as $\boldsymbol{b}_i$ and $\boldsymbol{f}_i$, respectively. We fix $\boldsymbol{s}$ and $\mathbf{C}$ such that $\mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*$, and compute $\Pr[|I| > \lambda \mid \mathbf{C}, \boldsymbol{s}]$. For simplicity, we omit the condition $\mathbf{C}$ and $\boldsymbol{s}$ below as they are fixed now. Then, according to our definition of I, we have for every $i \in [m]$:

$$\begin{aligned}
&\Pr_{\mathbf{B},\mathbf{F}}[i \in I] = \Pr_{\mathbf{B},\mathbf{F}}\left[\lfloor(\tilde{\mathbf{A}}\cdot\boldsymbol{s})_i\rceil_p \neq \lfloor(\mathbf{B}\cdot\mathbf{C}\cdot\boldsymbol{s} + \mathbf{F}\cdot(\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil))_i\rceil_p\right] \\
&= \Pr_{\boldsymbol{b}_i\boldsymbol{f}_i}\left[\left\lfloor\langle\mathbf{C}\cdot\boldsymbol{s},\boldsymbol{b}_i\rangle + \langle\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\rangle - \left\langle\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\right\rangle\right\rceil_p \neq \lfloor\langle\mathbf{C}\cdot\boldsymbol{s},\boldsymbol{b}_i\rangle + \langle\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\rangle\rceil_p\right] \\
&\leq \Pr_{\boldsymbol{b}_i\boldsymbol{f}_i}\left[\langle\mathbf{C}\cdot\boldsymbol{s},\boldsymbol{b}_i\rangle + \langle\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\rangle \in \mathsf{border}_{p,q,v}\left(\left|\left\langle\boldsymbol{e},\boldsymbol{f}_i\right\rangle\right|\right)\right] \qquad (16) \\
&= \sum_\tau \Pr_{\boldsymbol{f}_i}\left[\left|\left\langle\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\right\rangle\right| = \tau\right] \cdot \Pr_{\boldsymbol{b}_i\boldsymbol{f}_i}\left[\langle\mathbf{C}\cdot\boldsymbol{s},\boldsymbol{b}_i\rangle + \left\langle\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\right\rangle \in \mathsf{border}_{p,q,v}(\tau)\right] \\
&\leq \sum_\tau \Pr_{\boldsymbol{f}_i}\left[\left|\left\langle\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\right\rangle\right| = \tau\right] \cdot \frac{2\tau p}{q} \qquad (17) \\
&= \mathbf{E}_{\boldsymbol{f}_i}\left[\left|\left\langle\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\right\rangle\right|\right] \cdot \frac{2p}{q} \\
&\leq \beta\cdot\|\lfloor\boldsymbol{e}\rceil\|_1 \cdot \frac{2p}{q} \leq \beta\cdot\left(\|\boldsymbol{e}\|_1 + \frac{n}{2}\right)\cdot\frac{2p}{q} \qquad (18) \\
&\leq \frac{np\beta(\sigma+1)}{q} \leq \frac{1}{m}. \qquad (19)
\end{aligned}$$

where $v = \langle\boldsymbol{s}+\lfloor\boldsymbol{e}\rceil,\boldsymbol{f}_i\rangle - \lfloor\langle\boldsymbol{s}+\boldsymbol{e},\boldsymbol{f}_i\rangle\rfloor$ and (16) follows from the definition of a "border", (17) follows by Lemma 2.3 and the uniformity of $\langle\mathbf{C}\cdot\boldsymbol{s},\boldsymbol{b}_i\rangle$ over $\mathbb{Z}_q$, and (19) follows given the precondition $\|\boldsymbol{e}\| \leq n\sigma/2$, and each entry of $\boldsymbol{f}_i$ is bounded by β in absolute value.

From the above, we have that

$$\mathbf{E}[\ |I|\ ] = \sum_{i\in[m]} \mathbf{E}[\ i \in I\ ] = \sum_{i\in[m]} \Pr[\ i \in I\ ] \le 1.$$

Furthermore for $i \in [m]$, the events $i \in I$ are mutually independent, as their probabilities are based on independently chosen $\boldsymbol{b}_i$'s and $\boldsymbol{f}_i$'s. Therefore, by the Chernoff bound, we have

$$\Pr_{\mathbf{B},\mathbf{F}}\left[\ |I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^\ell\right)^*, \|\boldsymbol{e}\|_1 \le n\sigma/2\ \right] < 2^{-\lambda},$$

for any fixed $\boldsymbol{s}, \mathbf{C}, \boldsymbol{e}$ satisfying the condition. Using Equation (15) and the above calculation, we have

$$\Pr_{\mathbf{B},\mathbf{C},\mathbf{F},\boldsymbol{s},\boldsymbol{e}}[\ |I| > \lambda\ ] < \delta + 2^{-\ell+1} + 2^{-\lambda} + e^{-\left(\frac{\pi}{4}-\ln 2\right)n},$$

which completes the proof of Claim B.2. □

The bit-length of Z is $|I|(\log m + \log p)$, which is upper-bounded by $\lambda(\log m + \log p)$ with overwhelming probability, i.e., $1-\varepsilon = 1-\left(\delta + 2^{-\ell+1} + 2^{-\lambda} + e^{-\left(\frac{\pi}{4}-\ln 2\right)n}\right)$. Therefore, we have

$$\begin{aligned}
H_\infty^{\varepsilon'+\varepsilon}\left(f(\boldsymbol{s}) \mid \tilde{\mathbf{A}}, \lfloor\tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_p, \mathsf{aux}\right) &\ge H_\infty^{\varepsilon'+\varepsilon}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{s}+\lfloor\boldsymbol{e}\rceil, Z, \mathsf{aux}) \\
&\ge H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{s}+\lfloor\boldsymbol{e}\rceil, \mathsf{aux}) - \lambda(\log m + \log p) \\
&\ge H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \boldsymbol{s}+\lfloor\boldsymbol{e}\rceil, \mathsf{aux}) - \ell\log q - \lambda(\log m + \log p) \\
&\ge H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \boldsymbol{s}+\lfloor\boldsymbol{e}\rceil, \mathsf{aux}) - (\ell+\lambda)\log q \\
&\ge H_\infty^{\varepsilon'}(f(\boldsymbol{s}) \mid \boldsymbol{s}+\boldsymbol{e}, \mathsf{aux}) - (\ell+\lambda)\log q.
\end{aligned}$$

where the second and the third lines follow by Lemma 2.8 and Claim B.2, and the last line follows by $q \ge mp$. This completes the proof of Lemma B.1. □

Lemma B.3. *Let random variables $X_1, X_2, \cdots, X_n$ be i.i.d and follow D_σ where $\sigma > 0$ is a Gaussian parameter. For any $t > 0$, we have*

$$\Pr\left[\sum_{i=1}^n |X_k| \ge tn\sigma\right] \le 2^n \cdot e^{-\pi n t^2}.$$

Proof. For any i, consider the moment generating function of the random variable $|X_i|$

$$\mathbf{E}\left[e^{\theta|X_i|}\right] \le \mathbf{E}\left[e^{\theta|X_i|} + e^{-\theta|X_i|}\right] = \mathbf{E}\left[e^{\theta X_i} + e^{-\theta X_i}\right] = 2e^{\frac{\sigma^2\theta^2}{4\pi}}.$$

Then, for any parameter $\kappa > 0$, we have

$$\begin{aligned}
\Pr\left[\sum_{i=1}^n |X_i| \ge tn\sigma\right] &= \Pr\left[e^{\frac{\kappa}{n}\sum_{i=1}^n |X_i|} \ge e^{\kappa t}\right] \\
&\le e^{-\kappa t\sigma} \cdot \mathbf{E}\left[e^{\frac{\kappa}{n}\sum_{i=1}^n |X_i|}\right] \\
&= e^{-\kappa t\sigma} \cdot \prod_{i=1}^n \mathbf{E}\left[e^{\frac{\kappa}{n}|X_i|}\right] \\
&\le 2^n \cdot e^{\frac{\sigma^2\kappa^2}{4\pi n} - \kappa t\sigma},
\end{aligned} \tag{20}$$

where the inequality (20) comes from Markov's inequality. In order to let the term $\frac{\sigma^2\kappa^2}{4\pi n} - \kappa t\sigma$ reaches its minimum, we set $\kappa = \frac{2\pi nt}{\sigma}$, then we have

$$\Pr\left[\sum_{i=1}^{n} |X_i| \geq tn\sigma\right] \leq 2^n \cdot e^{-\pi nt^2},$$

which completes the proof. □

Comparison with Noise Lossiness Framework. It should be noted that we can also analyze the hardness of general entropic LWR by employing the *noise lossiness* framework [BD20a]. In brief, the conditional smooth entropy $H^{\epsilon}_{\infty}(\boldsymbol{s}|\tilde{\mathbf{A}},$
$\lfloor\tilde{\mathbf{A}}\boldsymbol{s}\rceil)$ can be similarly lower bounded by $H^{\epsilon}_{\infty}(\boldsymbol{s} \mid \boldsymbol{s}+\boldsymbol{e})$. This means that the noise lossiness framework is consistent with our framework from the perspective of feasibility.

For further comparison, especially the concrete lower bound of modulus, we need to compute the modulus constraint when applying the noise lossiness framework. Concretely, in the proof of Lemma 4.3, the inequality 5 is turned to upper bound $\mathbf{E}\left[\ |\langle \boldsymbol{f}_i, \boldsymbol{e}\rangle|\ \right]$ for β bounded $\boldsymbol{f}_i$ and Gaussian noise $\boldsymbol{e} \sim D^n_{\sigma}$. In order to apply the Chernoff bound lemma to give an upper bound for $\Pr[|I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^{\ell}\right)^*]$, we need each event $i \in I$ to be mutually independent, which indicates that fixing $\boldsymbol{e}$ before approximation of $\Pr[i \in I \mid \mathbf{C}\cdot\boldsymbol{s} \in \left(\mathbb{Z}_q^{n}\right)^*]$ is necessary. Thus, $\mathbf{E}[|\langle \mathbf{f}_i, \mathbf{e}\rangle|]$ can be bounded by $\beta \cdot \sum_i |e_i|$. Since each entry e_i of $\boldsymbol{e}$ is distributed according to D_{σ}, we can prove that $\Pr_{\mathbf{e}}[\sum_i |e_i| \geq nt] \leq 2^n \cdot \exp\left(-\frac{\pi nt^2}{\sigma^2}\right)$. Hence $\sum_i |e_i|$ has an upper bound $O(n\sigma)$ overwhelmingly, yielding that $\mathbf{E}[|\langle \mathbf{f}_i, \mathbf{e}\rangle|]$ can be bounded by $O\left(\frac{p\beta n\sigma}{q}\right)$. Therefore, q is with lower bound $O(nmp\beta\sigma)$. On the other hand, the lower bound itself of noise lossiness should also be considered. Specifically, for general entropic secrets, the noise lossiness is with lower bound $H_{\infty}(\boldsymbol{s}|\boldsymbol{s}+\boldsymbol{e})_g \geq H_{\infty}(\boldsymbol{s}) - n\log(\frac{q}{\sigma}) - 1$; for bounded entropic secrets, the noise lossiness is with lower bound $H_{\infty}(\boldsymbol{s}|\boldsymbol{s}+\boldsymbol{e})_b \geq H_{\infty}(\boldsymbol{s}) - \sqrt{2\pi n}\frac{r}{\sigma}\log e$, where r is the upper bound of ℓ_2 norm of secrets. For convenience of comparison, we relist the lower bound of q by our rounding lossiness approach, and the lower bounds of rounding lossiness for general and bounded entropic secrets as follows: $q > p^* \geq nmp\beta$, $H_{\infty}(\boldsymbol{s}|\lfloor\boldsymbol{s}\rceil_{q,p^*})_g \geq H_{\infty}(\boldsymbol{s}) - n\log p^*$, $H_{\infty}(\boldsymbol{s}|\lfloor\boldsymbol{s}\rceil_{q,p^*})_g \geq H_{\infty}(\boldsymbol{s}) - n\log(\frac{p^*\cdot\gamma}{q})$, where γ is the upper bound of ℓ_{∞} norm of secrets.

Based on these bounds, we can see that, for general entropic secrets, the modulus q of our framework is similar to the noise lossiness framework, if the two frameworks are required to have the same entropy lower bound. For bounded secrets, the modulus q of our framework can be saved at least a factor of $O(\sqrt{n})$ compared with the noise lossiness framework, if we minimize the entropy requirement of secrets of the two frameworks simultaneously. In other words, our approach can achieve better parameters than the noise lossiness approach. Besides, when working with certain secret distribution $\mathcal{S}$, rounding lossiness is easier to compute since the leakage is a determined function on $\boldsymbol{s}$.

To sum up, we find it more advantageous to work with our rounding lossiness framework compared with the *noise lossiness* presented in [BD20a].

C Hardness of Entropic MLWR

Definition C.1 (Lossy Sampler over Ring, Definition 5.13 in [LW20])**.** *Let n, ℓ, f, p, q, k be positive integers, $R = O_K$ be the ring of integers of a field extension K with degree n, and ϕ be a distribution over $K_{\mathbb{R}}$. We*

define the following efficient lossy sampler $\tilde{\mathbf{A}} \xleftarrow{\$} \mathsf{Lossy}(1^n, 1^\ell, 1^f, 1^k, q, \phi)$ *as:*

$\mathsf{Lossy}(1^n, 1^\ell, 1^f, 1^k, q, \phi)$: *Sample* $\mathbf{D} \xleftarrow{\$} (R_q)^{\ell \times f}$, $\mathbf{C} \xleftarrow{\$} (R_q)^{f \times k}$, $\mathbf{F} \xleftarrow{\$} \phi^{\ell \times k}$ *and output* $\tilde{\mathbf{A}} = \mathbf{D} \cdot \mathbf{C} + \mathbf{F}$.

The output of Lossy algorithm is computationally indistinguishable from uniformly random sample according to the following lemma and corollary.

Lemma C.2. *Let* $\mathbf{A} \xleftarrow{\$} (R_q)^{\ell \times k}$, *and let* $\tilde{\mathbf{A}} \xleftarrow{\$} \mathsf{Lossy}(1^n, 1^\ell, 1^f, 1^k, q, \phi)$. *Then, according to the module-*$\mathsf{RLWE}_{\ell,f,q,\phi}$ *assumption, we have:* $\mathbf{A} \overset{c}{\approx} \tilde{\mathbf{A}}$.

Corollary C.3. *Adopt the notations in Lemma 2.25 and Lemma C.2. Assuming the* $\mathsf{RLWE}_{\ell,q,\phi'}$ *problem is computationally hard, then* $\mathbf{A} \overset{c}{\approx} \tilde{\mathbf{A}}$.

We denote that vector $\boldsymbol{r} \in (R)^k$ *maximal belongs* to a factor $\mathcal{I}$ of qR, abbreviated as $\boldsymbol{r} \in_{\max} \mathcal{I}R$ if the following conditions hold.

- For every coordinate r_i of $\boldsymbol{r}$, we have $r_i \in \mathcal{I}R$.
- For any ideal $\mathcal{J} | qR$ such that $\mathcal{I} | \mathcal{J}$, there exists at least one coordinate r_j such that $r_j \notin \mathcal{J}R$.

Lemma C.4 ([LPR13])**.** *Let* $a \in R_q$ *and* $a \leftarrow \phi$ *for a* B_e*-bounded distribution* ϕ *under canonical embedding, let* $\mathbf{B}$ *be a basis of* R *with dual basis* $\mathbf{B}'$ *that has* B_d*-bounded* ℓ_∞ *norm for all coordinates, and* $b \in R_q$ *is arbitrary. Then writing* $a \cdot b = \langle \mathbf{B}, \boldsymbol{c} \rangle$ *for some integral vector* $\boldsymbol{c}$*, we have that* c_j *is* $B_e B_d \cdot \|b\|_2$*-bounded.*

Theorem C.5 (Hardness of Entropic Module-RLWR)**.** *Let* $\lambda, n, p, p^*, q, \ell, f, k$ *be positive integers,* $R = O_K$ *be the ring of integers of a number field* $K = \mathbb{Q}(\alpha)$ *with degree* n, $\mathbf{B}$ *be a basis of* R *with* B_{d_1} *bounded* ℓ_∞ *norm for all entries, all entries of its dual basis* $\mathbf{B}'$ *be* B_{d_2}*-bounded in* ℓ_∞ *norm,* ϕ *be a* β*-bounded distribution over* $K_\mathbb{R}$ *for some real* $\beta > 0$*, such that* $q > p^* \geq B_{d_1} B_{d_2} \beta k \ell p n^{\frac{5}{2}}$ *and* $\gcd(q, [O_K : \mathbb{Z}[\alpha]]) = 1$. *Then there exists a poly-time reductions from module-*$\mathsf{RLWE}_{\ell,f,q,\phi}$ *to* $\mathsf{ent\text{-}dMLWR}(q, p, \mathbf{B}, k, m, \mathcal{S})$*, where* $\mathcal{R}_{q,p^*}(\mathcal{S} \bmod \mathfrak{q}) \geq (2n + \ell + \lambda) \log q + \omega(\log \lambda)$ *for any prime ideal factor* $\mathfrak{q}$ *of* qR.

Lemma C.6. *Adopt the parameters and conditions in Theorem C.5: let* λ n, p, p^*, $q, \ell, k, \beta, B_{d_1}, B_{d_2}$ *be positive integers,* $R = O_K$ *be the ring of integers of a number field* K *with dimension* n *with basis* $\mathbf{B}$ *of* R*, and* ϕ *be a distribution over* $K_\mathbb{R}$*. Let* $(\boldsymbol{s}, \mathsf{aux})$ *be a pair of correlated random variables such that* $\Pr[\ \boldsymbol{s} \notin_{\max} \langle 1 \rangle\ ] < \delta$*. Let* $\tilde{\mathbf{A}}$ *be a vector independently output by the algorithm* $\mathsf{Lossy}(1^n, 1^\ell, 1^f, 1^k, q, \phi)$. *Then, for any* $\varepsilon' > 0$ *and security parameter* λ, $\varepsilon = \delta + \frac{n}{2^{f-1}} + 2^{-\lambda}$*, it holds:*

$$H_\infty^{\varepsilon' + \varepsilon}\left(\boldsymbol{s} \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}, \mathsf{aux}\right) \geq H_\infty^{\varepsilon'}(\boldsymbol{s} \mid \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*}, \mathsf{aux}) - (n + \lambda) \log q. \tag{21}$$

Proof. According to Definition C.1, $\tilde{\mathbf{A}}$ can be written as $\tilde{\mathbf{A}} = \mathbf{D} \cdot \mathbf{C} + \mathbf{F}$, then $\lfloor \tilde{\mathbf{A}} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p} = \lfloor \mathbf{D} \cdot \mathbf{C} \cdot \boldsymbol{s} + \mathbf{F} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}$. Moreover, $\lfloor \mathbf{D} \cdot \mathbf{C} \cdot \boldsymbol{s} + \mathbf{F} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}$ can be written as

$$\lfloor \mathbf{D} \cdot \mathbf{C} \cdot \boldsymbol{s} + \mathbf{F} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p} = \left\lfloor \mathbf{D} \cdot \mathbf{C} \cdot \boldsymbol{s} + \frac{q}{p^*} \mathbf{F} \cdot \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*} + \frac{q}{p^*} \mathbf{F} \left(\frac{p^*}{q} \boldsymbol{s} - \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*} \right) \right\rfloor_{\mathbf{B},p}.$$

We define the set $I \overset{\text{def}}{=} \left\{ (i,j) \in [\ell] \times [n] : \left\lfloor \left(\mathbf{D} \cdot \mathbf{C} \cdot \boldsymbol{s} + \frac{q}{p^*} \mathbf{F} \cdot \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*} \right)_i [j] \right\rceil_p \neq \left\lfloor \left(\tilde{\mathbf{A}} \cdot \boldsymbol{s} \right)_i [j] \right\rceil_p \right\}$, where $(\boldsymbol{x})_i[j]$ denotes the jth coefficient of ith coordinate of $\boldsymbol{x}$ relative to $\mathbf{B}$. Let $Z = \left\{ \left((i,j), \left\lfloor \left(\tilde{\mathbf{A}} \cdot \boldsymbol{s} \right)_i [j] \right\rceil_p \right) : (i,j) \in I \right\}$,

and it is not hard to see that $(\tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p})$ can be reconstructed completely given $\mathbf{D}, \mathbf{C}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*} \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*}, Z$. Therefore:

$$H_\infty^{\varepsilon'+\varepsilon}(\boldsymbol{s} \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}, \mathsf{aux}) \geq H_\infty^{\varepsilon'+\varepsilon}\left(\boldsymbol{s} \mid \mathbf{C}, \mathbf{D}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*} \lfloor \boldsymbol{s} \rceil_{\mathbf{B},p^*}, Z, \mathsf{aux}\right).$$

Next, we show a lower bound for the right hand side by bounding the min-entropy loss given Z. To do this, we first bound the probability that the size of I is large:

Claim C.7. $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda] < \delta + \frac{n}{2^{f-1}} + 2^{-\lambda}$.

Proof. We divide the event $|I| > \lambda$ into two cases: $\boldsymbol{s} \in_{\max} \langle 1 \rangle$ and $\boldsymbol{s} \notin_{\max} \langle 1 \rangle$:

$$\begin{aligned}
\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda] &= \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \notin_{\max} \langle 1 \rangle] \cdot \Pr_{\boldsymbol{s}}[\boldsymbol{s} \notin_{\max} \langle 1 \rangle] && (22)\\
&\quad + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle] \cdot \Pr_{\boldsymbol{s}}[\boldsymbol{s} \in_{\max} \langle 1 \rangle] && (23)\\
&\leq \Pr_{\boldsymbol{s}}[\boldsymbol{s} \notin_{\max} \langle 1 \rangle] + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle] && (24)\\
&< \delta + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle]. && (25)
\end{aligned}$$

It remains to bound $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle]$. In order to compute $\Pr[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle]$, we divide the condition into two cases: $\mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle$ and $\mathbf{C} \cdot \boldsymbol{s} \notin_{\max} \langle 1 \rangle$. Then we have:

$$\begin{aligned}
&\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle]\\
&= \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle] \cdot \Pr_{\mathbf{C},\boldsymbol{s}}[\mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle]\\
&+ \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \notin_{\max} \langle 1 \rangle] \cdot \Pr_{\mathbf{C},\boldsymbol{s}}[\mathbf{C} \cdot \boldsymbol{s} \notin_{\max} \langle 1 \rangle \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle].
\end{aligned}$$

Combining equations 22, we have

$$\begin{aligned}
\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda] &< \delta + \Pr_{\mathbf{C},\boldsymbol{s}}[\mathbf{C} \cdot \boldsymbol{s} \notin_{\max} \langle 1 \rangle] + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle]\\
&< \delta + \frac{n}{2^{f-1}} + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle].
\end{aligned} \tag{26}$$

Finally, it remains to bound $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle]$. It is easy to verify that $\mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle$ implies $\boldsymbol{s} \in_{\max} \langle 1 \rangle$, so $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \boldsymbol{s} \in_{\max} \langle 1 \rangle, \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle] = \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle]$. On the other hand, for uniformly random matrix $\mathbf{D} \in (R_q)^{\ell \times f}$ and $\mathbf{C}\boldsymbol{s} \in_{\max} \langle 1 \rangle$, it's easy to verify $\mathbf{D} \cdot \mathbf{C}\boldsymbol{s}$ is uniformly at random by similar arguments as Theorem 5.7 in [LW20].

Now we claim that $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle] < 2^{-\lambda}$. To show this, we fix any $\boldsymbol{s}$ and $\mathbf{C}$ such that $\mathbf{C} \cdot \boldsymbol{s} \in_{\max} \langle 1 \rangle$, and compute $\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[|I| > \lambda \mid \mathbf{C}, \boldsymbol{s}]$. For simplicity, below we omit the condition $\boldsymbol{s}, \mathbf{C}$ as they are fixed now.

We denote the i-th row of the matrices $\mathbf{D}$ and $\mathbf{F}$ as as $\boldsymbol{d}_i$ and $\boldsymbol{f}_i$, respectively, and omit the common basis $\mathbf{B}$ in the subscript of rounding function for simplicity. For the definition of I, we have that for every

$(i,j) \in [\ell] \times [n]$:

$$\begin{aligned}
&\Pr_{\mathbf{D},\mathbf{F}}[\ (i,j) \in I\ ] = \Pr_{\mathbf{D},\mathbf{F}}\left[\ \left\lfloor \left(\mathbf{D}\cdot\mathbf{C}\boldsymbol{s} + \frac{q}{p^*}\mathbf{F}\cdot\lfloor \boldsymbol{s}\rceil_{p^*}\right)_i [j]\right\rceil_p \neq \left\lfloor (\tilde{\mathbf{A}}\cdot\boldsymbol{s})_i [j]\right\rceil_p \ \right] \\
&= \Pr_{\boldsymbol{d}_i,\boldsymbol{f}_i}\left[\ \left\lfloor \left(\langle \mathbf{C}\boldsymbol{s}, \boldsymbol{d}_i\rangle + \frac{q}{p^*}\langle \boldsymbol{f}_i, \lfloor \boldsymbol{s}\rceil_{p^*}\rangle\right)[j]\right\rceil_p \neq \left\lfloor \left(\langle \mathbf{C}\boldsymbol{s}, \boldsymbol{d}_i\rangle + \frac{q}{p^*}\langle \boldsymbol{f}_i, \lfloor \boldsymbol{s}\rceil_{p^*}\rangle\right)[j] + \frac{q}{p^*}\left\langle \boldsymbol{f}_i, \frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s}\rceil_{p^*}\right\rangle [j]\right\rceil_p \ \right] \\
&\leq \Pr_{\boldsymbol{d}_i,\boldsymbol{f}_i}\left[\ \left(\langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{d}_i\rangle + \frac{q}{p^*}\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\rangle\right)[j] \in \mathsf{border}_{p,q,\nu}\left(\left|\frac{q}{p^*}\left\langle \boldsymbol{f}_i, \frac{p^*}{q}\boldsymbol{s} - \lfloor \boldsymbol{s}\rceil_{p^*}\right\rangle [j]\right|\right)\ \right] \qquad (27) \\
&= \sum_{\tau}\Pr_{\boldsymbol{f}_i}\left[\ \left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle [j]\right| = \tau\ \right]\Pr_{\boldsymbol{d}_i}\left[\ \left(\langle \mathbf{C}\cdot\boldsymbol{s}, \boldsymbol{d}_i\rangle + \frac{q}{p^*}\left\langle \lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle\right)[j] \in \mathsf{border}_{p,q,\nu}(\tau)\ \right] \qquad (28) \\
&\leq \sum_{\tau}\Pr_{\boldsymbol{f}_i}\left[\ \left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle [j]\right| = \tau\ \right]\cdot\frac{2\tau p}{q} \qquad (29) \\
&= \mathbf{E}_{\boldsymbol{f}_i}\left[\ \left|\left\langle \boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}, \boldsymbol{f}_i\right\rangle [j]\right|\ \right]\cdot\frac{2p}{q} \\
&\leq \frac{B_{d_1}B_{d_2}\beta n^{3/2}kp}{p^*} \leq \frac{1}{\ell n}, \qquad (30)
\end{aligned}$$

where (27) follows from the definition of a "border", (28) follows from the formula of total probability, (29) follows by the size of a "border" in Lemma 2.3 and the uniformity of $\langle \boldsymbol{d}_i, \mathbf{C}\boldsymbol{s}\rangle[j]$ over $\mathbb{Z}_q$, and (30) follows from the Lemma C.4, since each entry of $\boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*}$ has $\frac{q}{2p^*}$-bounded ℓ_∞ norm with respect to $\mathbf{B}$, then the ℓ_2-norm of $(\boldsymbol{s} - \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{p^*})_i$ is $\frac{q}{2p^*}B_{d_1}n^{3/2}$-bounded by Cauchy-Schwarz inequality, and each entry of $\boldsymbol{f}$ is bounded by β under the canonical imbedding.

From the above calculation, we can derive that

$$\mathbf{E}[|I|] = \sum_{(i,j)\in[\ell]\times[n]}\mathbf{E}[(i,j)\in I] = \sum_{(i,j)\in[\ell]\times[n]}\Pr[(i,j)\in I] < 1.$$

(Recall that $(i,j) \in I$ is a binary event). We note that for $(i,j) \in [\ell]\times[n]$, the events $(i,j)\in I$ are mutually independent, as $\boldsymbol{d}_i$ and $\boldsymbol{f}_i$ are independently chosen, and $\langle \boldsymbol{d}_i, \mathbf{C}\boldsymbol{s}\rangle$ is uniformly random over R_q thus each coefficient of it is independent to others. Therefore, by the Chernoff bound, we have $\Pr_{\mathbf{B},\mathbf{F}}[\ |I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in_{\max} \langle 1\rangle\ ] < 2^{-\lambda}$, for any fixed $\boldsymbol{s}, \mathbf{C}$ satisfying the condition.

Using Equation (26) and the above calculation, we have

$$\Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[\ |I| > \lambda\ ] < \delta + \frac{n}{2^{f-1}} + \Pr_{\mathbf{D},\mathbf{C},\mathbf{F},\boldsymbol{s}}[\ |I| > \lambda \mid \mathbf{C}\cdot\boldsymbol{s} \in_{\max}\langle 1\rangle\ ] < \delta + \frac{n}{2^{f-1}} + 2^{-\lambda}.$$

This proves the claim. □

The bit-length of Z is $|I|(\log(\ell n) + \log p)$, which is upper-bounded by $\lambda(\log(\ell n) + \log p)$ with over-

whelming probability, i.e., $1-\varepsilon = 1-(\delta + \frac{n}{2^{f-1}} + 2^{-\lambda})$ (as the Lemma statement). Therefore, we have

$$\begin{aligned}
H_\infty^{\varepsilon'+\varepsilon}\left(\boldsymbol{s} \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}}\cdot \boldsymbol{s}\rceil_{\mathbf{B},p}, \mathsf{aux}\right) &\geq H_\infty^{\varepsilon'+\varepsilon}\left(\boldsymbol{s} \mid \mathbf{C}, \mathbf{D}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}, Z, \mathsf{aux}\right) \\
&\geq H_\infty^{\varepsilon'}\left(\boldsymbol{s} \mid \mathbf{C}, \mathbf{D}, \mathbf{F}, \mathbf{C}\boldsymbol{s}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}, \mathsf{aux}\right) - \lambda(\log(\ell n) + \log p) \\
&\geq H_\infty^{\varepsilon'}\left(\boldsymbol{s} \mid \mathbf{C}, \mathbf{D}, \mathbf{F}, \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}, \mathsf{aux}\right) - n\log q - \lambda(\log(\ell n) + \log p) \\
&\geq H_\infty^{\varepsilon'}\left(\boldsymbol{s} \mid \frac{q}{p^*}\lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}, \mathsf{aux}\right) - (n+\lambda)\log q \\
&= H_\infty^{\varepsilon'}(\boldsymbol{s} \mid \lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}, \mathsf{aux}) - (n+\lambda)\log q,
\end{aligned}$$

where the second and the third lines follow from Lemma 2.8 and Claim C.7, and the last line follows from the fact $q \geq \ell n p$. This completes the proof. □

Now we can prove Theorem C.5 as follows:

Theorem C.5. Our target is to prove the following: under module-$\mathsf{RLWE}_{\ell,f,q,\phi}$ assumption with parameters in the theorem, we have

$$\left(\begin{bmatrix}\mathbf{A}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \mathbf{A}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s}\rangle \rceil_{\mathbf{B},p}\end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix}\mathbf{A}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \mathbf{A}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor u\rceil_{\mathbf{B},p}\end{bmatrix} \right) \tag{31}$$

where $\mathbf{A} \xleftarrow{\$} (R_q)^{\ell\times k}, \boldsymbol{a} \xleftarrow{\$} (R_q)^k, \boldsymbol{s} \xleftarrow{\$} \mathcal{S} \subseteq (R_q)^k, u \xleftarrow{\$} R_p$.

By Lemma C.2, we can replace $\mathbf{A}$ with $\tilde{\mathbf{A}}$ to obtain

$$\left(\begin{bmatrix}\mathbf{A}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \mathbf{A}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s}\rangle \rceil_{\mathbf{B},p}\end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix}\tilde{\mathbf{A}}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \tilde{\mathbf{A}}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s}\rangle \rceil_{\mathbf{B},p}\end{bmatrix} \right)$$

By Lemma C.6, for $\varepsilon = 2^{-\lambda} + \delta + \frac{n}{2^{f-1}}$ and any $\varepsilon' > 0$, we have:

$$\begin{aligned}
H_\infty^{\varepsilon'+\varepsilon}(\boldsymbol{s} \bmod \mathfrak{q} \mid \tilde{\mathbf{A}}, \lfloor \tilde{\mathbf{A}}\cdot\boldsymbol{s}\rceil_{\mathbf{B},p}) &\geq H_\infty^{\varepsilon'}(\boldsymbol{s} \bmod \mathfrak{q} \mid \lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}) - (\ell+\lambda)\log(q) \\
&\geq (2n+\ell+\lambda)\cdot\log(q) + \omega(\log(\lambda)) - (\ell+\lambda)\log(q) \\
&\geq 2n\log(q) + \omega(\log(\lambda)).
\end{aligned}$$

On the other hand, it's clear that $H_\infty(\boldsymbol{s} \bmod \mathfrak{q}) \geq H_\infty(\boldsymbol{s} \bmod \mathfrak{q} \mid \lfloor \boldsymbol{s}\rceil_{\mathbf{B},p^*}) \geq (2n+\ell+\lambda)\cdot\log(q) + \omega(\log(\lambda))$ for any prime ideal factor $\mathfrak{q}$ of qR. Then by union bound,

$$\begin{aligned}
\Pr_{\boldsymbol{s}}[\ \boldsymbol{s} \notin_{\max} \langle 1\rangle\ ] \leq \Pr_{\boldsymbol{s}}[\exists \text{ prime } \mathfrak{q} \mid qR : \boldsymbol{s} \bmod \mathfrak{q} = \mathbf{0}] &\leq \sum_{\text{prime } \mathfrak{q}} \Pr[\boldsymbol{s} \bmod \mathfrak{q} = \mathbf{0}] \\
&\leq n\log q \cdot q^{-(2n+\ell+\lambda)} \cdot 2^{-\omega(\log\lambda)} < q^{-\lambda},
\end{aligned}$$

Therefore, δ can be set as $q^{-\lambda}$, and thus $\varepsilon = 2^{-\lambda} + q^{-\lambda} + 2^{-\ell+1}$.

Combining above with leftover hash lemma as Corollary 2.36 we have:

$$\left(\begin{bmatrix}\tilde{\mathbf{A}}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \tilde{\mathbf{A}}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor \langle \boldsymbol{a}, \boldsymbol{s}\rangle \rceil_{\mathbf{B},p}\end{bmatrix} \right) \overset{s}{\approx} \left(\begin{bmatrix}\tilde{\mathbf{A}}\\ \boldsymbol{a}\end{bmatrix}, \begin{bmatrix}\lfloor \tilde{\mathbf{A}}\boldsymbol{s}\rceil_{\mathbf{B},p}\\ \lfloor u\rceil_{\mathbf{B},p}\end{bmatrix} \right).$$

The exact statistical distance is bounded by $2^{-\omega(\log\lambda)}$. Finally, we replace the lossy $\tilde{\mathbf{A}}$ with uniformly random $\mathbf{A}$ to get:

$$\left(\begin{bmatrix} \tilde{\mathbf{A}} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \tilde{\mathbf{A}}\boldsymbol{s} \rceil_{\mathbf{B},p} \\ \lfloor u \rceil_{\mathbf{B},p} \end{bmatrix} \right) \overset{c}{\approx} \left(\begin{bmatrix} \mathbf{A} \\ \boldsymbol{a} \end{bmatrix}, \begin{bmatrix} \lfloor \mathbf{A}\boldsymbol{s} \rceil_{\mathbf{B},p} \\ \lfloor u \rceil_{\mathbf{B},p} \end{bmatrix} \right).$$

Combining the above three hybrids proves (31). By a simple hybrid argument as [AKPW13], we can further prove the desired statement

$$(\mathbf{A}, \lfloor \mathbf{A}\boldsymbol{s} \rceil_{\mathbf{B},p}) \overset{c}{\approx} (\mathbf{A}, \lfloor \boldsymbol{u} \rceil_{\mathbf{B},p}).$$

□